(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월17일
(11) 등록번호 10-1737299
(24) 등록일자 2017년05월11일

(51) 국제특허분류(Int. Cl.)
*H04L 9/06* (2006.01) *H04L 9/12* (2006.01)
(52) CPC특허분류
*H04L 9/0637* (2013.01)
*H04L 9/0662* (2013.01)
(21) 출원번호 10-2017-7006321
(22) 출원일자(국제) 2015년08월07일
심사청구일자 2017년03월10일
(85) 번역문제출일자 2017년03월07일
(65) 공개번호 10-2017-0036100
(43) 공개일자 2017년03월31일
(86) 국제출원번호 PCT/EP2015/025056
(87) 국제공개번호 WO 2016/020068
국제공개일자 2016년02월11일
(30) 우선권주장
1414007.3 2014년08월07일 영국(GB)
(56) 선행기술조사문헌
US07076064 B2
US20060056625 A1

(73) 특허권자
**구루로직 마이크로시스템스 오이**
핀란드 투르쿠 20100 린난카투 34
(72) 발명자
**케르크케이넨 투오마스**
핀란드 20320 튀르쿠 라우탈란카투 2 비17
(74) 대리인
**김태홍, 김진희**

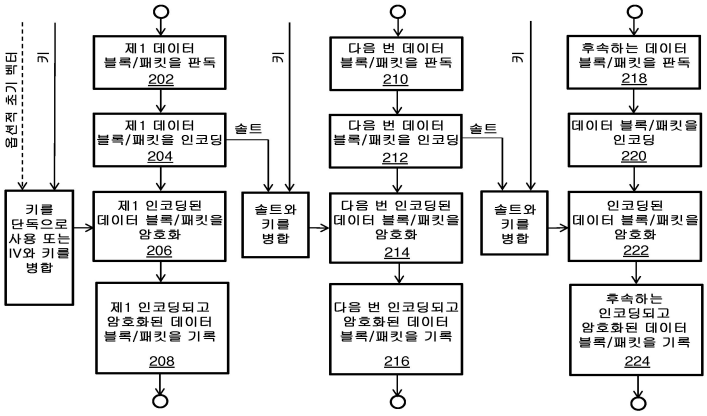
전체 청구항 수 : 총 42 항 심사관 : 김상인

(54) 발명의 명칭 **인코더, 디코더 및 방법**

## (57) 요 약

대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하는 방법이 제공된다. 제1 인코딩된 데이터 블록을 생성하기 위해, 입력 데이터(D1) 중 적어도 제1 데이터 블록이 인코딩된다. 그 다음, 적어도 제1 인코딩된 데이터 블록은, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록을 제공하기 위해, 적어도 하나의 키를 사용하여 암호화된다. 또한, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록을 제공하기 위해, 다음 번 인코딩된 데이터를 암호화함에 있어서 사용하기 위한 제1 제1 시드 값이 생성된다. 또한, 입력 데이터(D1)의 각각의 데이터 블록이 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록을 암호화함에 있어서 사용하기 위한 다음 번 시드 값이 순차 반복적 방식으로 생성된다.

## 대 표 도



(52) CPC특허분류
***H04L 9/12*** (2013.01)
*H04L 2209/125* (2013.01)

# 명 세 서

## 청구범위

### 청구항 1

복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더(110)로서,

상기 인코더(110)는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 상기 입력 데이터(D1)를 프로세싱하기 위한 데이터 프로세싱 장치(data processing arrangement)를 포함하고, 상기 데이터 프로세싱 장치는 상기 인코딩되고 암호화된 데이터(E2)를 생성하기 위한 인코딩 및 암호화 프로세스를 통합하고,

(i) 상기 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 상기 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 인코딩하도록, 그리고 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 하나의 키를 사용하여 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하도록 동작 가능하고;

(ii) 상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번(next) 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 제1 시드 값(seed value)을 생성하도록 동작가능하고;

(iii) 상기 데이터 프로세싱 장치는, 상기 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 상기 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식(sequential repetitive manner)으로 생성하도록 동작가능하고,

인코딩되고 암호화될 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성되는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더(110).

### 청구항 2

제1항에 있어서,

상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 상기 적어도 하나의 키를 동작 중에 제공받는 것을 특징으로 하는 인코더(110).

### 청구항 3

제1항 또는 제2항에 있어서,

상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 동작가능한 것을 특징으로 하는 인코더(110).

### 청구항 4

제1항에 있어서,

상기 데이터 프로세싱 장치는, 상기 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 동작가능한 것을 특징으로 하는 인코더(110).

### 청구항 5

제1항에 있어서,

상기 데이터 프로세싱 장치는, 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(initialization vector; IV)를 채용하도록 동작가능한 것을 특징으로 하는 인코더(110).

**청구항 6**

제1항에 있어서,

상기 데이터 프로세싱 장치는, 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 상기 인코딩되고 암호화된 데이터(E2)에 포함시키도록 동작가능한 것을 특징으로 하는 인코더(110).

**청구항 7**

제1항에 있어서,

상기 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 인코딩 및 암호화의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 인코딩되고 암호화된 데이터(E2)를 상기 순차 반복적 방식으로 생성하기 위해 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능한 것을 특징으로 하는 인코더(110).

**청구항 8**

제1항에 있어서,

상기 데이터 프로세싱 장치는, 1차원 데이터, 다차원 데이터, 텍스트 데이터, 이진 데이터, 센서 데이터, 오디오 데이터, 이미지 데이터, 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능한 것을 특징으로 하는 인코더(110).

**청구항 9**

제1항에 있어서,

상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 인코더(110)로부터의 전달을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 동작가능한 것을 특징으로 하는 인코더(110).

**청구항 10**

제9항에 있어서,

상기 암호화된 통신 연결은, 보안 소켓 레이어(Secure Sockets Layer; SSL)/전송 레이어 보안(Transport Layer Security; TLS) 프로토콜을 통해 구현되는 것을 특징으로 하는 인코더(110).

**청구항 11**

제1항에 있어서,

상기 데이터 프로세싱 장치는, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(reduced instruction set computing; RISC) 프로세서를 채용하는 것에 의해 구현되는 것을 특징으로 하는 인코더(110).

**청구항 12**

인코더(110)를 통해, 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법으로서,

상기 인코더(110)는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 상기 입력 데이터(D1)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 상기 데이터 프로세싱 장치는 상기 인코딩되고 암호화된 데이터

(E2)를 생성하기 위한 인코딩 및 암호화 프로세스를 통합하고,

상기 방법은,

(i) 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 상기 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 제1 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 인코딩하는 단계;

(ii) 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 하나의 키를 사용하여 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하는 단계;

(iii) 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 제1 시드 값을 생성하는 단계; 및

(iv) 상기 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 상기 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하는 단계를 포함하고,

인코딩되고 암호화될 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성되는 것을 특징으로 하는 것을 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 13**

제12항에 있어서,

상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 상기 적어도 하나의 키를 상기 데이터 프로세싱 장치에 제공하는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 14**

제12항 또는 제13항에 있어서,

상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 15**

제12항에 있어서,

상기 방법은, 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 16**

제12항에 있어서,

상기 방법은, 상기 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 17**

제12항에 있어서,

상기 방법은, 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한

시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 상기 인코딩되고 암호화된 데이터(E2)에 포함시키도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 18**

제12항에 있어서,

상기 방법은, 연관된 시드 값을 사용하여 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 인코딩 및 암호화의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 인코딩되고 암호화된 데이터(E2)를 상기 순차 반복적 방식으로 생성하기 위해 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 19**

제12항에 있어서,

상기 방법은, 1차원 데이터, 다차원 데이터, 텍스트 데이터, 이진 데이터, 센서 데이터, 오디오 데이터, 이미지 데이터, 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 20**

제12항에 있어서,

상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 인코더(110)로부터의 전달을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 21**

제20항에 있어서,

상기 방법은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 상기 암호화된 통신 연결을 구현하는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 22**

제12항에 있어서,

상기 방법은, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 상기 데이터 프로세싱 장치를 구현하는 단계를 포함하는 것을 특징으로 하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법.

**청구항 23**

복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더(120)로서,

상기 디코더(120)는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 상기 인코딩되고 암호화된 데이터(E2)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 상기 디코더(120)는 상기 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받고, 상기 데이터 프로세싱 장치는 상기 디코딩된 데이터(D3)를 생성하기 위한 디코딩 및 암호해제 프로세스를 통합하고,

(i) 상기 데이터 프로세싱 장치는, 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 상기 적어도 하나의 키를 사용하여 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하도록, 그리고 디코딩된 데이터(D3)에 포함시키기 위한 적어도 제1 디코딩된 데이터 블록 또는

데이터 패킷 또는 데이터 스트림을 제공하기 위해 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하도록 동작가능하고;

(ii) 상기 데이터 프로세싱 장치는, 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제함에 있어서 사용하기 위한 제1 시드 값을 생성하도록, 그리고 상기 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 상기 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하도록 동작가능하고;

(iii) 상기 데이터 프로세싱 장치는, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 상기 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 후속하는 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하도록 동작가능하고,

암호해제되고 디코딩될 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성되는 것을 특징으로 하는 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더(120).

**청구항 24**

제23항에 있어서

상기 데이터 프로세싱 장치는, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 25**

제23항 또는 제24항에 있어서,

상기 데이터 프로세싱 장치는, 상기 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 26**

제23항에 있어서,

상기 데이터 프로세싱 장치는, 상기 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 27**

제23항에 있어서,

상기 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 암호해제 및 디코딩의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 디코딩된 데이터(D3)를 상기 순차 반복적 방식으로 생성하기 위해 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 28**

제23항에 있어서,

상기 데이터 프로세싱 장치는, 인코딩되고 암호화된 1차원 데이터, 인코딩되고 암호화된 다차원 데이터, 인코딩되고 암호화된 텍스트 데이터, 인코딩되고 암호화된 이진 데이터, 인코딩되고 암호화된 센서 데이터, 인코딩되

고 암호화된 오디오 데이터, 인코딩되고 암호화된 이미지 데이터, 인코딩되고 암호화된 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 29**

제23항에 있어서,

상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 디코더(120)에서의 수신을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 동작가능한 것을 특징으로 하는 디코더(120).

**청구항 30**

제29항에 있어서,

상기 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현되는 것을 특징으로 하는 디코더(120).

**청구항 31**

제23항에 있어서,

상기 데이터 프로세싱 장치는, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 구현되는 것을 특징으로 하는 디코더(120).

**청구항 32**

디코더(120)를 통해, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법으로서,

상기 디코더(120)는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 상기 인코딩되고 암호화된 데이터(E2)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 상기 디코더(120)는 상기 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받고, 상기 데이터 프로세싱 장치는 상기 디코딩된 데이터(D3)를 생성하기 위한 디코딩 및 암호해제 프로세스를 통합하고,

상기 방법은,

(i) 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 상기 적어도 하나의 키를 사용하여 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하는 단계;

(ii) 상기 디코딩된 데이터(D3)에 포함시키기 위한 적어도 제1 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하는 단계;

(iii) 상기 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 제1 시드 값을 생성하는 단계; 및

(iv) 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 상기 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 후속하는 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하는 단계를 포함하고,

암호해제되고 디코딩될 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성되는 것을 특징으로 하는 인코딩되고 암

호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 33**

제32항에 있어서,

상기 방법은, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 34**

제32항 또는 제33항에 있어서,

상기 방법은, 상기 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 35**

제32항에 있어서,

상기 방법은, 상기 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 36**

제32항에 있어서,

상기 방법은, 연관된 시드 값을 사용하여 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 암호해제 및 디코딩의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 디코딩된 데이터(D3)를 상기 순차 반복적 방식으로 생성하기 위해 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 37**

제32항에 있어서,

상기 방법은, 인코딩되고 암호화된 1차원 데이터, 인코딩되고 암호화된 다차원 데이터, 인코딩되고 암호화된 텍스트 데이터, 인코딩되고 암호화된 이진 데이터, 인코딩되고 암호화된 센서 데이터, 인코딩되고 암호화된 오디오 데이터, 인코딩되고 암호화된 이미지 데이터, 인코딩되고 암호화된 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 38**

제32항에 있어서,

상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 디코더(120)에서의 수신을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함하는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 39**

제38항에 있어서,

상기 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현되는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 40**

제32항에 있어서,

상기 데이터 프로세싱 장치는, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 구현되는 것을 특징으로 하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법.

**청구항 41**

제1항에 기재된 적어도 하나의 인코더(110), 및 제23항에 기재된 적어도 하나의 디코더(120)를 포함하는 코덱(130).

**청구항 42**

비일시적 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 판독가능 명령어를 포함하는 컴퓨터 프로그램으로서,

상기 컴퓨터 판독가능 명령어는, 제12항 또는 제32항에 기재된 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능한, 비일시적 컴퓨터 판독가능 저장 매체를 포함하는, 컴퓨터 프로그램.

**청구항 43**

삭제

**청구항 44**

삭제

## *발명의 설명*

### *기 술 분 야*

[0001] 본 개시는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더, 및 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하는 대응하는 방법에 관한 것이다. 또한, 본 개시는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더, 및 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 대응하는 방법에 관한 것이다. 또한, 본 개시는, 컴퓨터 판독가능 명령어가 저장된 비일시적 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품에 관한 것인데, 컴퓨터 판독가능 명령어는 상기 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다. 추가적으로, 본 개시는 적어도 하나의 상기 언급된 인코더 및 적어도 하나의 상기 언급된 디코더를 포함하는 코덱에 관한 것이다.

### *배 경 기 술*

[0002] 일반적으로, 용어 "암호화(encryption)"는, 인가된 당사자만이 메시지 또는 정보를 판독할 수 있는 방식으로 메시지 또는 정보를 인코딩하는 프로세스를 가리킨다. 암호화를 다루는 과학의 분야는 암호학으로 칭해진다. 역사적으로 정보는 암호화되어 왔으며, 각각의 암호화 알고리즘은 그 고유의 관련된 취약점을 갖는다는 것이 널리 알려져 있다. 암호학의 한 분야인 암호해독법(cryptanalysis)은 암호화 알고리즘에서의 취약점을 찾기 위해 사용된다.

[0003] 암호화 알고리즘은 대칭 알고리즘(즉, 대칭 키 알고리즘) 및 비대칭 알고리즘(즉, 비대칭 키 알고리즘)으로 분류될 수 있다. 대칭 및 비대칭 알고리즘은, 암호화 키가 사용되고 프로세싱되는 방식이 상호 상이하다. 대칭 암호화 알고리즘은 송신단(transmitting end)에서 데이터를 암호화하기 위해 그리고 대응하는 수신단(receiving end)에서 암호화된 데이터를 암호해제하기 위해 공유된 공통 키를 사용한다. 한편, 비대칭 암호화 알고리즘은 두 개의 상이한 키를 사용하는데, 그 중 하나는 데이터를 암호화하기 위해 사용되는 공개 키(public key)이고

나머지 하나는 암호화된 데이터를 암호해제하기 위해 사용되는 개인 키(private key)이다. 오직 공개 키만이 당사자 사이에서 공유된다.

[0004] 또한, 일 방향의 메시지 다이제스트 함수(one-way message digest function), 즉 해시 함수(hash function)가 존재하는데, 해시 함수가 나타내는 데이터가 복원하기 어렵고 불가능하기 때문에, 그런 만큼, 해시 함수는 데이터 암호화 기술이 아니다. 그러나, 일 방향의 메시지 다이제스트 함수는, 데이터 및 패스워드의 진위를 검증하기 위해 사용되며, 또한 암호화 알고리즘을 위한 암호화 키를 생성하기 위해 사용된다.

[0005] 데이터 암호화는, 많은 컴퓨팅 리소스를 필요로 하는 기술적으로 까다로운 연산이다는 것이 널리 알려져 있다. 따라서, 컴퓨팅 리소스를 절약하기 위해 그리고 컴퓨팅 시간을 감소시키기 위해, 비대칭 및 대칭 암호화 알고리즘의 하이브리드 조합이 종종 사용된다. 이것은 충분히 강력한 보호를 제공하며, 그 결과 인가되지 않은 제3자의 암호해제는 현재의 컴퓨팅 리소스로는 실시간으로 실행될 수 없다. 이러한 종류의 접근 방식은, 예를 들면, 보안 소켓 레이어(Secure Sockets Layer; SSL)/전송 레이어 보안(Transport Layer Security; TLS) 및 보안 쉘(Secure Shell; SSH)과 같은 다양하고 상이한 데이터 전송 프로토콜에서, 그리고 예를 들면, 프리티 굳 프라이버시(Pretty Good Privacy; PGP)와 같은 이메일 메시지에 서명하고 암호화하는 애플리케이션에서 일반적으로 사용된다.

[0006] 암호학, 즉 암호 및 암호해독법의 과학적 연구는, 암호해독법의 수단을 통해 암호화 알고리즘에서의 취약점을 찾기 위해 시도하는 계속해서 발전하고 있는 과학의 분야이다는 것이 입증되었다. 이 이유 때문에, 정보를 최대한 보호할 수 있는 것이 필수적이지만, 그러나 대응하여, 암호화를 구현하기 위해 사용되는 컴퓨팅 리소스의 사용에 관한 타협을 이룰 필요성이 존재한다. 또한, 이용가능한 컴퓨팅 리소스는 일반적으로 제한되며, 배터리 전력을 절약하기 위해 최대로 노력을 기울이는 모바일 디바이스에서는 특히 제한된다.

[0007] 미국 특허문헌 US2006/0188095A1(Jung 등등; "Combination encoding method for simultaneous encrypting and channel encoding, transmitting apparatus thereof, combination decoding method for simultaneous channel decoding and decrypting, and receiving apparatus thereof"; 삼성전자(Samsung Electronics Co., Ltd.)에 양도됨)에서는, 조합 인코딩 방법, 그 송신 장치, 조합 디코딩 방법, 및 그 수신 장치가 설명된다. 송신 장치는, 소스 코딩 메시지에 대해 조합 인코딩을 수행하고 조합 인코딩된 메시지를 출력하고, 그에 의해 암호화 및 채널 인코딩을 동시에 수행하기 위한 조합 인코딩 유닛을 포함한다. 수신 장치는, 복조기로부터의 노이즈가 부가된 조합 인코딩된 메시지에 대해 조합 디코딩을 수행하고 소스 코딩 메시지를 출력하고, 그에 의해 노이즈가 부가된 조합 인코딩된 메시지에 대해 채널 디코딩 및 암호해제를 동시에 수행하기 위한 조합 디코딩 유닛을 포함한다.

[0008] 미국 특허문헌 US 8660261 B2(Chang 등등; "System and apparatus for integrated video/image encoding/decoding and encryption/decryption"; 미디어텍 싱가폴 유한 책임 회사(Mediatek Singapore Pte., Ltd.)에 양도됨)에서는, 멀티미디어 코덱에 대한 암호화 대응 엔트로피 코더가 설명된다. 엔트로피 코더는, 다수의 세트의 허프만(Huffman) 테이블을 리드 온리 메모리(read-only memory; ROM)에 저장하지 않으면서 랜덤화된 허프만 코딩 스킴(scheme)을 구현한다. 엔트로피 코더는 단일 세트의 코드 테이블을 저장하는 ROM, 테이블 룩업을 수행하는 것에 의해 심볼을 원래의 코드 워드로 변환하거나 그 반대로 변환하는 ROM에 커플링된 테이블 룩업 섹션, 및 동형 코드 생성기 알고리즘(isomorphic code generator algorithm)을 사용하여, 원래의 허프만 코드 워드를 랜덤화된 허프만 코드 워드로 변환하거나 그 반대로 변환하기 위한 테이블 랜덤화기(randomizer) 섹션을 포함한다. 테이블 랜덤화기 섹션은, 암호화/암호해제 키를 사용하여 의사랜덤 비트 생성기에 의해 생성되는 키 호핑 시퀀스(key hopping sequence)에 기초하여 변환을 수행한다.

미국 특허문헌 US2006/0056625A1(Sumie 등등; "Encryption method, encryption apparatus, data storage distribution apparatus and data delivery system" 히타치 가스가이 일렉트릭사(Kokusai Electric, Inc.)에 양도됨)에서는, 입력 파라미터로부터 고유하게 결정된 난수 시퀀스를 생성하는 난수 생성 유닛에 의해 생성된 난수 시퀀스를 이용하여 암호화 대상 데이터를 데이터를 암호화하는 암호화 방법이 개시며, 이 방법은 암호화 대상 데이터의 메타데이터에 기초하여 입력 파라미터를 생성하는 단계를 포함한다.

공개된 논문(Samarakoon 등등; "Encrypted video over TETRA")에서는, 보안성이 개선된 모바일 통신 시스템을 기술하고 있다. 이 시스템은 무선 인터페이스 암호화 외에 엔드 투 엔드(end to end) 암호화를 사용한다. 이 시스템은 엔드 투 엔드 암호화에 동기화를 제공하기 위해 프레임 삽입 기술을 사용한다. 프레임 삽입 기술은 데이터 손실을 피하기 위해 연속 비디오 프레임들 사이에 있는 전송된 비디오 스트림에 동기화 프레임을 삽입한다. 그러나, 삽입을 허용하려면, 애플리케이션이 동일한 전체 전송 레이트를 유지하기 위해 데이터 레이트를 줄어야

한다.

## 발명의 내용

[0009] 본 개시는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더를 제공하는 것을 목적으로 한다.

[0010] 또한, 본 개시는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더를 제공하는 것을 목적으로 한다.

[0011] 제1 양태에서, 본 개시의 실시형태는, 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더를 제공하는데, 인코더는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 데이터 프로세싱 장치가, 상기 인코딩되고 암호화된 데이터(E2)를 생성하기 위한 인코딩 및 암호화 프로세스를 통합하는 것을 특징으로 하고,

[0012] (i) 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 인코딩하도록, 그리고 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 하나의 키를 사용하여 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하도록 동작 가능하고;

[0013] (ii) 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 제1 시드 값(seed value)을 생성하도록 동작 가능하고;

[0014] (iii) 데이터 프로세싱 장치는, 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식(sequential repetitive manner)으로 생성하도록 동작가능하고,

인코딩되고 암호화될 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 그 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성된다.

[0015] 본 발명은, 시드 값의 사용을 통해 대응하는 인코딩된 데이터를 생성하기 위해 데이터를 인코딩하기 위한 인코더의 향상된 형태를 제공할 수 있다는 이점을 갖는다.

[0016] 또한, 옵션적으로(optionally), 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 인코딩 및 암호화의 복수의 동시적 시퀀스로 분기하는 것에 의해 대응하는 인코딩되고 암호화된 데이터(E2)를 순차 반복적 방식으로 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능하다.

[0017] 옵션적으로, 인코더의 데이터 프로세싱 장치는, 하기에서 상세히 설명되는 바와 같이 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(reduced instruction set computing; RISC) 프로세서를 채용하는 것에 의해 구현된다.

[0018] 옵션적으로, 인코더의 데이터 프로세싱 장치는, 1차원 데이터, 다차원 데이터, 텍스트 데이터, 이진 데이터, 센서 데이터, 오디오 데이터, 이미지 데이터, 비디오 데이터(이들로 제한되지는 않음) 중 적어도 하나의 형태로 제공되는 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능하다.

[0019] 옵션적으로, 인코더의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받는다.

[0020] 옵션적으로, 인코더의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위한 시드 값과 조합하여 적어도 하나의 키를 반복적으로 사용하도록 동작가능하다. 대안적으로, 옵션적으로, 인코더의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위해 적어도 하나의 키를 단독으로 사용하

도록 동작가능하다.

[0021] 또한, 옵션적으로, 인코더의 데이터 프로세싱 장치는 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(initialization vector; IV)를 채용하도록 동작가능하다.

[0022] 또한, 옵션적으로, 인코더의 데이터 프로세싱 장치는, 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 인코딩되고 암호화된 데이터(E2)에 포함시키도록 동작가능하다.

[0023] 또한, 옵션적으로, 인코더의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 적어도 하나의 키의 전달을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 동작가능하다. 옵션적으로, 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현된다.

[0024] 제2 양태에서, 본 개시의 실시형태는, 인코더를 통해, 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하는 방법을 제공하는데, 인코더는 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 데이터 프로세싱 장치가, 상기 인코딩되고 암호화된 데이터(E2)를 생성하기 위한 인코딩 및 암호화 프로세스를 통합하는 것을 특징으로 하고, 상기 방법은,

[0025] (i) 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 제1 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 인코딩하는 단계;

[0026] (ii) 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 하나의 키를 사용하여 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하는 단계;

[0027] (iii) 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 제1 시드 값을 생성하는 단계; 및

[0028] (iv) 복수의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하는 단계를 포함하고,

인코딩되고 암호화될 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 그 주어진 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성된다.

옵션적으로, 상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 상기 적어도 하나의 키를 상기 데이터 프로세싱 장치에 제공하는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 상기 인코딩되고 암호화된 데이터(E2)에 포함시키도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 연관된 시드 값을 사용하여 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 인코딩 및 암호화의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 인코딩되고 암호화된 데이터(E2)를 상기 순차 반복적 방식으로 생성하기 위해 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 1차원 데이터, 다차원 데이터, 텍스트 데이터, 이진 데이터, 센서 데이터, 오디오 데이터, 이미지 데이터, 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 입력 데이터(D1)를 인코딩하고 암호화하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 인코더로부터의 전달을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다. 또 옵션적으로, 상기 방법은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 상기 암호화된 통신 연결을 구현하는 단계를 포함한다.

옵션적으로, 상기 방법은, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 상기 데이터 프로세싱 장치를 구현하는 단계를 포함한다.

[0029] 제3 양태에서, 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는 상기 언급된 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다.

[0030] 제4 양태에서, 본 개시의 실시형태는, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더를 제공하는데, 디코더는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 디코더는 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받고, 데이터 프로세싱 장치가, 상기 디코딩된 데이터(D3)를 생성하기 위한 디코딩 및 암호해제 프로세스를 통합하는 것을 특징으로 하며,

[0031] (i) 데이터 프로세싱 장치는, 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 적어도 하나의 키를 사용하여 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하도록, 그리고 디코딩된 데이터(D3)에 포함시키기 위한 적어도 제1 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하도록 동작가능하고;

[0032] (ii) 데이터 프로세싱 장치는, 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제함에 있어서 사용하기 위한 제1 시드 값을 생성하도록, 그리고 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 다음 번 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하도록 동작가능하고; 그리고

[0033] (iii) 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 후속하는 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하도록 동작가능하고,

암호해제되고 디코딩될 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성된다.

[0034] 또한, 옵션적으로, 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 암호해제 및 디코딩의 복수의 동시적 시퀀스로 분기하는 것에 의해 대응하는 디코딩된 데이터(D3)를 순차 반복적 방식으로 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고

디코딩하도록 동작가능하다.

[0035] 옵션적으로, 디코더의 데이터 프로세싱 장치는, 하기에 상세히 설명되는 바와 같이 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 RISC 프로세서를 채용하는 것에 의해 구현되고; 이러한 RISC 프로세서는, 상대적으로 더 간단한 사슬연결된 연산(concatenated operation)을 아주 빠른 속도로 수행할 수 있고, 스트리밍 포맷으로 제공되는 데이터를, 예를 들면, 실시간으로 인코딩하고 디코딩하는 데 적합하다.

[0036] 옵션적으로, 디코더의 데이터 프로세싱 장치는, 인코딩되고 암호화된 1차원 데이터, 인코딩되고 암호화된 다차원 데이터, 인코딩되고 암호화된 텍스트 데이터, 인코딩되고 암호화된 이진 데이터, 인코딩되고 암호화된 센서 데이터, 인코딩되고 암호화된 오디오 데이터, 인코딩되고 암호화된 이미지 데이터, 인코딩되고 암호화된 비디오 데이터(이들로 제한되지는 않음) 중 적어도 하나의 형태로 제공되는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 동작가능하다.

[0037] 옵션적으로, 디코더의 데이터 프로세싱 장치는 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받는다.

[0038] 옵션적으로, 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위한 시드 값과 조합하여 적어도 하나의 키를 반복적으로 사용하도록 동작가능하다. 대안적으로, 옵션적으로, 데이터 프로세싱 장치는, 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위해 적어도 하나의 키를 단독으로 사용하도록 동작가능하다.

[0039] 또한, 옵션적으로, 데이터 프로세싱 장치는, 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 동작가능하다.

옵션적으로, 상기 데이터 프로세싱 장치는, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 디코더에서의 수신을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 동작가능하다. 또 옵션적으로, 상기 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현된다.

[0040] 제5 양태에서, 본 개시의 실시형태는, 디코더를 통해, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 방법을 제공하는데, 디코더는 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함하고, 디코더는 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받고, 데이터 프로세싱 장치는 상기 디코딩된 데이터(D3)를 생성하기 위한 디코딩 및 암호해제 프로세스를 통합하고, 상기 방법은,

[0041] (i) 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 생성하기 위해 적어도 하나의 키를 사용하여 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하는 단계;

[0042] (ii) 디코딩된 데이터(D3)에 포함시키기 위한 적어도 제1 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 적어도 제1 인코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 디코딩하는 단계;

[0043] (iii) 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 제공하기 위해 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 다음 번 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 제1 시드 값을 생성하는 단계; 및

[0044] (iv) 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림이 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림 중 후속하는 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하고 디코딩함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하는 단계를 포함하며,

암호해제되고 디코딩될 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 대해, 상기 주어진 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 이전의 디코딩된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림에 기초하여 시드 값이 생성된다.

옵션적으로, 상기 방법은, 상기 복수의 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위한 시드 값과 조합하여 상기 적어도 하나의 키를 반복적으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제하기 위해 상기 적어도 하나의 키를 단독으로 사용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 적어도 제1 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림을 암호해제할 때 상기 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 연관된 시드 값을 사용하여 인코딩되고 암호화된 데이터 블록 또는 데이터 패킷 또는 데이터 스트림의 암호해제 및 디코딩의 복수의 동시적 시퀀스로 분기하는 것에 의해 상기 대응하는 디코딩된 데이터(D3)를 상기 순차 반복적 방식으로 생성하기 위해 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 인코딩되고 암호화된 1차원 데이터, 인코딩되고 암호화된 다차원 데이터, 인코딩되고 암호화된 텍스트 데이터, 인코딩되고 암호화된 이진 데이터, 인코딩되고 암호화된 센서 데이터, 인코딩되고 암호화된 오디오 데이터, 인코딩되고 암호화된 이미지 데이터, 인코딩되고 암호화된 비디오 데이터 중 적어도 하나의 형태로 제공되는 상기 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다.

옵션적으로, 상기 방법은, 상기 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 상기 적어도 하나의 키의 상기 디코더에서의 수신을, 수동으로 또는 암호화된 이메일을 통해 또는 암호화된 통신 연결을 통해, 조정하도록 상기 데이터 프로세싱 장치를 동작시키는 단계를 포함한다. 또 옵션적으로, 상기 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현된다.

옵션적으로, 상기 데이터 프로세싱 장치는, 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 구현된다.

[0045] 제6 양태에서, 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는 상기 언급된 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다.

[0046] 제7 양태에서, 본 개시의 실시형태는, 상기 언급된 인코더 및 상기 언급된 디코더를 포함하는 코덱을 제공한다.

[0047] 상기 언급된 방법은, 대응하는 암호화 알고리즘을 사용하는 종래 기술의 방법으로 달성되는 보호와 비교하여, 상당한 보호 향상을 가능하게 한다. 본 개시의 실시형태에 따른 방법은, 어떤 암호화 알고리즘이 사용되는지에 무관하게, 임의의 적절한 인코딩 솔루션을 사용하여 구현될 수 있다. 이렇게 함에 있어서, 이들 방법은 통합된 암호화 알고리즘의 거동을 변경하지는 않는데, 이것은, 통합된 암호화 알고리즘에 의해 제공되는 보호가 손상되지 않는다는 것을 의미한다. 따라서, 본 개시의 실시형태에 따른 방법은, 종래 기술의 데이터 압축 및 암호화 알고리즘을 더 강화한다.

[0048] 또한, 상기 언급된 방법은, 일반적으로 널리 알려진 오프 소스 또는 독점적(proprietary) 데이터 압축 소프트웨어 애플리케이션, 예컨대 7-Zip 또는 Win-Zip, 및 등등("7-Zip" 및 "Win-Zip"은 독점적 상표이다)과 연계하여 구현될 수 있다.

[0049] 또한, 인코딩 및 암호화 프로세스의 통합은, 멀티프로세싱에 대한, 또는 여러 프로세스를 병렬 방식으로 실행시키기 위한 효율적인 모델을 제공한다. 통합은, 이용가능한 컴퓨팅 능력에 따른 주어진 중앙 프로세싱 유닛(Central Processing Unit; CPU) 및 주어진 그래픽 프로세싱 유닛(Graphical Processing Unit; GPU)에 대한 최적의 프로세싱 구조의 구현을 가능하게 한다. 따라서, 상기 언급된 방법은, 입력 데이터(D1)의 데이터 블록 및/또는 데이터 패킷이, 인코딩 프로세스가 실행하고 있는 시스템 및/또는 플랫폼의 CPU 및 GPU에 대해 최적인 포맷으로 최적화될 때, 인코딩 프로세스에서의 통합된 암호화 프로세스의 효율적인 스레딩을 가능하게 한다.

[0050] 상기 언급된 방법은, 아주 빠르지만, 여전히 효율적인 암호화 알고리즘을 사용하는 것을 가능하게 만든다. 이와 관련하여, 상기 언급된 방법은, 암호화 알고리즘 자체의 내부 동작과의 간섭 없이, 암호화 알고리즘을 효율적으로 사용한다. 상기 언급된 방법을 통한 구현에 적합한 암호화 알고리즘의 예는, AES, Twofish, Blowfish,

DES(Data Encryption Standard), Triple DES(3-DES), Serpent, IDEA(International Data Encryption Algorithm), MARS, RC6(Rivest Cipher 6), Camellia, CAST-128, Skipjack, XTEA(extended Tiny Encryption Algorithm), 및 등등(이들 예는 등록 상표를 포함한다)을 포함하지만, 그러나 이들로 제한되지는 않는다.

[0051] 또한, 암호화 프로세스를 인코딩 프로세스와 통합하는 추가적인 이점은, 이렇게 생성되는 인코딩되고 암호화된 데이터(E2)가, 예를 들면, 가상 사설 네트워크(Virtual Private Network; VPN) 터널링, 보안 쉘(SSH), 또는 SSL/TLS 프로토콜을 채용하는 보호된 보안 네트워크 연결을 갖는 네트워크를 통해 전송될 필요가 없다는 것이다. 따라서, 상기 언급된 방법은, 예를 들면, 공공 인터넷 네트워크에서 또는 웹서비스 및 클라우드 서비스에서 텍스트, 이진(binary), 오디오, 이미지, 비디오 및 다른 타입의 데이터를 송신하기 위한 유익한 모델을 제공한다.

[0052] 본 개시의 추가적인 양태, 이점, 특징 및 목적은, 후속하는 첨부의 청구범위와 연계하여 해석되는 예시적인 실시형태의 상세한 설명 및 도면으로부터 명확하게 될 것이다.

[0053] 본 개시의 특징은, 첨부의 청구범위에 의해 정의되는 바와 같은 본 개시의 범위를 벗어나지 않으면서, 다양한 조합으로 결합될 수 있다는 것이 인식될 것이다.

## *도면의 간단한 설명*

[0054] 앞서 언급한 개요뿐만 아니라, 예시적인 실시형태의 다음의 상세한 설명은 첨부된 도면들과 함께 판독되는 경우 더 잘 이해된다. 본 개시를 예시화하는 목적을 위해, 본 개시의 예시적인 구성이 도면에서 도시된다. 그러나, 본 개시는 본원에서는 개시되는 특정한 방법 및 장치로 제한되지 않는다. 또한, 기술 분야의 숙련된 자는 도면이 일정한 비율이 아니다는 것을 이해할 것이다. 가능한 경우마다, 동일한 도면 부호는 동일한 도면 부호에 의해 표기되었다.

이제, 단지 예시로서, 본 개시의 실시형태가 첨부의 도면을 참조로 설명될 것인데, 도면에서,

도 1은, 본 개시의 실시형태에 따른, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더 및 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더의 개략적인 예시인데, 인코더 및 디코더는 공동으로 코덱을 형성한다.

도 2는, 본 개시의 실시형태에 따른, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하는 제1 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다.

도 3은, 본 개시의 실시형태에 따른, 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 제2 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다.

도 4는, 본 개시의 다른 실시형태에 따른, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하는 제3 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다.

도 5는, 본 개시의 다른 실시형태에 따른, 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 제4 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다.

첨부된 도면에서 밑줄이 그어진 숫자는, 밑줄이 그어진 숫자가 배치되는 아이템 또는 밑줄이 그어진 숫자가 인접하는 아이템을 나타내기 위해 사용된다. 밑줄이 그어지지 않은 숫자는, 밑줄이 그어지지 않은 숫자를 아이템에 연결하는 라인에 의해 식별되는 아이템이다. 숫자에 밑줄이 그어지지 않고 관련된 화살표가 부수하는 경우, 밑줄이 그어지지 않은 숫자는, 화살표가 가리키고 있는 일반적인 아이템을 식별하기 위해 사용된다.

## *발명을 실시하기 위한 구체적인 내용*

[0055] 하기의 상세한 설명은 본 개시의 실시형태 및 본 개시의 실시형태가 구현될 수 있는 방식을 예시한다. 본 개시를 수행하는 최상의 모드가 개시되지만, 기술 분야의 숙련된 자는, 본 개시를 수행하기 위한 또는 실시하기 위한 다른 실시형태도 가능하다는 것을 인식할 것이다.

[0056] 개요에서, 본 개시의 실시형태는, 인코더로 통합되는 데이터 암호화 방법, 필요한 부분만 수정한(mutatis mutandis), 디코더로 통합되는 데이터 암호해제 방법에 관한 것이다. 상기 언급된 통합된 암호화 방법을 사용하여 인코더에 의해 인코딩되고 암호화되는 데이터는, 관련된 디코더로의 유사한 통합을 채용하지 않고는, 암호해

제 및 디코딩될 수 없다.

[0057] 본 개시에 있어서, 사용되고 있는 주어진 인코더의 인코딩 프로세스로 통합되는 암호화 프로세스가 설명된다. 이것은, 암호화 프로세스에 의해 채용되는 암호화 알고리즘의 성능 및 능력을 약하게 하지 않으면서, 관련된 암호화를 상당히 강력하게 만든다. 상기 언급된 통합 방법은 이미 알려진 암호화 알고리즘을 유익하게 사용한다. 암호화 프로세스의 통합은, 옵션적으로, 데이터 블록 및/또는 데이터 패킷을 인코딩하는 그리고 1차원 또는 다차원 텍스트, 이진, 오디오, 이미지, 비디오 또는 다른 타입의 데이터를 프로세싱하는 인코더에서 구현된다.

[0058] 본 개시의 실시형태는, 암호화 알고리즘의 복잡성을 감소시키고, 그에 의해 데이터 프로세서에 의해 소비되는 컴퓨팅 리소스 및 프로세싱 에너지를 절약함으로써, 데이터를 암호화하는 비용 효율적인 방식을 제공하는 것을 목적으로 한다. 또한, 동일한 암호화 알고리즘 설정을 통해, 본 개시의 실시형태는 종래 기술의 솔루션보다 상당히 더 강력한 보호를 제공한다. 이것은, 예를 들면, 더 나은 데이터 보호 레벨을 달성하기 위해 여분의 컴퓨팅 리소스를 추가할 필요가 없을 것이다는 것을 의미한다.

[0059] 암호화되지 않은 정보가 "평문(plaintext)"으로 칭해지고, 대응하여, 본 개시 내용 전반에 걸쳐 암호화된 정보가 "비문(ciphertext)"으로 칭해진다는 것이 기술 분야의 숙련된 자에게는 명백할 것이다.

[0060] 도 1을 참조하면, 본 개시의 실시형태는 다음에 관한 것이다.

[0061] (i) 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하기 위한 인코더(110), 및 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하는 대응하는 방법;

[0062] (ii) 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 디코더(120), 및 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 대응하는 방법; 및

[0063] (iii) 적어도 하나의 인코더 및 적어도 하나의 디코더의 조합, 즉 인코더(110) 및 디코더(120)의 조합을 포함하는 코덱(130).

[0064] 옵션적으로, 디코딩된 데이터(D3)는, 연산의 무손실 모드에서와 같이, 입력 데이터(D1)와 정확히 동일하다. 대안적으로, 옵션적으로, 디코딩된 데이터(D3)는, 연산의 손실 모드에서와 같이, 입력 데이터(D1)와 거의 유사하다. 여전히 대안적으로, 옵션적으로, 디코딩된 데이터(D3)는, 예를 들면, 변환 방식에 의해 입력 데이터(D1)와 상이하지만, 그러나 입력 데이터(D1)에 존재하는 실질적으로 유사한 정보를 유지한다; 예를 들면, 디코딩된 데이터(D3)는, 예를 들면, 상이한 타입의 통신 플랫폼, 소프트웨어 레이어, 통신 디바이스, 및 등등과 호환가능하게 되도록 디코딩된 데이터(D3)의 재포맷팅이 또한 필요로 되는 경우에, 입력 데이터(D1)와는 상이한 것으로 유용하게 만들어진다.

[0065] 인코더(110)는, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해 입력 데이터(D1)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함한다. 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 하기에 상세히 설명되는 바와 같이 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 축약형 명령어 세트 컴퓨팅(RISC) 프로세서를 채용하는 것에 의해 구현되고; 이러한 RISC 프로세서는, 상대적으로 더 간단한 사슬연결된 연산을 아주 빠른 속도로 수행할 수 있고, 스트리밍 포맷으로 제공되는 데이터를, 예를 들면, 실시간으로 인코딩하고 디코딩하는 데 적합하다.

[0066] 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 1차원 데이터, 다차원 데이터, 텍스트 데이터, 이진 데이터, 센서 데이터, 오디오 데이터, 이미지 데이터, 비디오 데이터(이들로 제한되지는 않음) 중 적어도 하나의 형태로 제공되는 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능하다. 입력 데이터(D1)는 복수의 데이터 블록 및/또는 데이터 패킷을 포함한다. 옵션적으로, 입력 데이터(D1)는 데이터의 스트림, 또는 데이터 파일로서 수신된다.

[0067] 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받는다. 대안적으로, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는 적절한 키 생성 알고리즘을 사용하여 적어도 하나의 키를 생성하도록 동작가능하다.

[0068] 인코더(110)의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 복수의 데이터 블록 및/또는 데이터 패킷 중 제1 데이터 블록 및/또는 데이터 패킷을 인코딩하도록 동작가능하다. 그 다음, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코

딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 적어도 하나의 키를 사용하여 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하도록 동작가능하다.

[0069] 또한, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화함에 있어서 사용하기 위한 제1 시드 값을 생성하도록 동작가능하다. 계속해서, 인코더(110)의 데이터 프로세싱 장치는, 복수의 데이터 블록 및/또는 데이터 패킷이 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하도록 동작가능하다.

[0070] 옵션적으로, 복수의 데이터 블록 및/또는 데이터 패킷은, 하나씩 차례로 단계적으로, 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화된다, 즉, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 형태로 인코딩되고 암호화된다.

[0071] 인코더(110)의 기술적 구현은, 인코딩 프로세스 및 암호화 프로세스를 수행하기 위해 각각 사용되는 인코딩 알고리즘 및 암호화 알고리즘에 따라 변할 수도 있다는 것이 인식될 것이다. 그럼에도 불구하고, 기술적 구현은 인코딩 및 암호화 프로세스를 통합한다. 다시 말하면, 선택된 암호화 알고리즘은 인코더(110)에 유용하게 포함될 것이다는 것, 즉 임베딩될 것이다는 것이 인식될 것이다.

[0072] 통합은, 인코딩 및 암호화될 각각의 후속하는 데이터 블록 및/또는 데이터 패킷에 대한 시드 값을, 그 이전의 데이터 블록 및/또는 데이터 패킷에 기초하여 생성하는 것을 목표로 한다. 결과적으로, 각각의 인코딩되고 암호화된 데이터 및/또는 데이터 패킷의 후속하는 암호해제는, 그 이전의 인코딩되고 암호화된 데이터 및/또는 데이터 패킷의 암호해제 및 디코딩에 의존한다, 즉 하기에서 상세히 설명되는 바와 같이 순차 반복적 방식으로 의존한다. 무단 침입하는 공격자가, 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하기 위한 가능한 솔루션을 발견할 수 있기 위해서는, 인코더(110) 및 디코더(120) 둘 다의 완전한 기능성을 생성해야 할 것이기 때문에, 시드 값을 채용하는 것에 의한 암호화의 이러한 순차 반복적 방식은 암호화 알고리즘의 효과를 향상시킨다.

[0073] 대안적인 구현예에서는, 주어진 데이터 블록 및/또는 데이터 패킷이 먼저 암호화되고, 그 다음 인코딩되고 암호화된 데이터(E2)로 인코딩될 수 있다. 그러나, 암호화 이전에 데이터 블록 및/또는 데이터 패킷의 인코딩을 수행하는 것은, 입력 데이터(D1)가, 이전의 데이터 블록 및/또는 데이터 패킷과 비교하여, 후속하는 데이터 블록 및/또는 데이터 패킷에서, 즉 이전의 데이터 블록 및/또는 데이터 패킷의 부분적인 또는 전체 사본에서 종종 많은 작은 변화를 포함하기 때문에, 유익하다는 것이 인식될 것이다. 따라서, 인코더(110)의 데이터 프로세싱 장치는, 입력 데이터(D1)의 복수의 데이터 블록 및/또는 데이터 패킷을 복수의 인코딩된 데이터 블록 및/또는 데이터 패킷으로 인코딩하는 적절한 데이터 중복 제거 기술(data de-duplication technique)을 채용하도록 동작가능하다. 하나의 예로서, 복수의 데이터 블록 및/또는 데이터 패킷을 인코딩하기 위해, GB 1411451.6에서 설명되는 방법이 사용될 수 있다. 다른 예로서, 복수의 데이터 블록 및/또는 데이터 패킷을 인코딩하기 위해, GB 1411531.5에서 설명되는 방법이 사용될 수 있다.

[0074] 또한, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 복수의 인코딩된 데이터 블록 및/또는 데이터 패킷이 암호화되기 이전에 또는 암호화된 이후에, 복수의 인코딩된 데이터 블록 및/또는 데이터 패킷에 대해 추가적인 인코딩 프로세스를 수행하도록 동작가능하다. 이 목적을 위해, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 엔트로피 수정 인코딩(entropy-modifying encoding), 델타 인코딩(delta encoding), ODelta 인코딩, 1u 또는 8u 범위 인코딩(range encoding), 런 렝쓰 인코딩(Run Length Encoding; RLE), 스플릿 RLE(Split RLE; SRLE), 및/또는 보간 인코딩(interpolation encoding) 중 하나를 채용하도록 동작가능하다. 본원에서, 용어 "델타 인코딩"은, 완전한 데이터 파일 대신 순차적인 데이터 사이의 차이의 형태로 데이터를 저장 또는 송신하는 방식을 가리키고, 한편 용어 "ODelta"는, 예를 들면, 참조에 의해 본원에 통합되는 특허문헌 GB 1303661.1에서 설명되는 바와 같이, 이진 카운팅 체제(binary counting regime)에서의 랩어라운드(wraparound)에 기초한 인코딩의 차동 형태를 가리킨다. 용어 "SRLE" 또는 "스플릿 RLE"는, 특허문헌 GB 1303660.3에서 설명되는 바와 같은 스플릿 런 렝쓰 인코딩 방법을 가리킨다.

[0075] 한 예에서, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 하나 이상의 적절한 엔트로피 수정 인코딩 방법을 채용하는 것에 의해, 암호화 이전에 복수의 인코딩된 데이터 블록 및/또는 데이터 패킷을 추가로 압축하도록 동작가능하다.

[0076] 한 예로서, Gurulogic Microsystems Oy로부터 입수가능한 구루로직 다변량 코덱(Gurulogic Multi-Variate

Codec; GMVC®) 코딩 솔루션이 유용하게 사용된다. GMVC®는 상이한 타입의 데이터를 아주 효율적으로 인코딩할 수 있고, 동시에, 원래 입력, 즉 입력 데이터(D1)의 전체 정보를 포함하는 여러 개의 상이한 데이터 스트림을 엔트로피 인코딩 방식으로 효율적으로 생성할 수 있다. 예를 들면, 상기 언급된 독점적 GMVC® 코딩 솔루션에서, 이미지 데이터 또는 비디오 데이터의 인코딩은, 특허문헌 GB 2503295A("Encoder and method") 및 GB 2505169A("Decoder and method")에서 설명되는 바와 같이, 입력 데이터(D1)의 컨텐츠에 따라, 다양하고 상이한 데이터 스트림을 생성하기 위해 상호 상이한 방법을 채용한다. 따라서, 인코딩되고 암호화된 데이터(E2)를 생성하기 위해서는, 암호화 이전에, 입력 데이터(D1)의 엔트로피 및 비트 카운트를 고려하면서, 상이한 타입의 데이터가, 정확하게 그 타입의 데이터에 대해 최적화된 상이한 엔트로피 인코더를 사용하여 효율적으로 압축되는 것이 유익하다.

[0077] 이와 관련하여, 옵션적으로, 인코더(110)의, 예를 들면 하나 이상의 상기 언급된 RISC 프로세서를 사용하여 구현되는, 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 데이터 블록 및/또는 데이터 패킷의 인코딩 및 암호화의 복수의 동시적 시퀀스로 분기하는 것에 의해 대응하는 인코딩되고 암호화된 데이터(E2)를 순차 반복적 방식으로 생성하기 위해 입력 데이터(D1)를 인코딩하고 암호화하도록 동작가능하다; 이러한 RISC 프로세서는 상대적으로 더 간단한 사슬연결된 연산을 아주 빠른 속도로 수행할 수 있고, 스트리밍 포맷으로 제공되는 데이터를, 예를 들면, 실시간으로 인코딩 및 디코딩하는 데 적합하다. 이것은, 입력 데이터(D1)의 더 빠른 프로세싱을 제공하기 위해 여러 개의 동시적 프로세스를 병렬로 실행하는 것을 허용할뿐만 아니라, 향상된 암호화 보안도를 제공하는 것을 허용하는데, 그 이유는, 인코딩되고 암호화된 데이터(E2)를 디코딩할 때, 디코더(120)가 유사한 형태의 분기를 채용하는 것을 필요로 하기 때문이다.

[0078] 옵션적으로, 분기를 구현하기 위해, 입력 데이터(D1)는, 예를 들면, 입력 데이터(D1)에서 존재하는 데이터의 각각의 타입에 대해, 데이터 블록 및/또는 데이터 패킷의 상이한 스트림으로 세분된다. 유익하게는, 상이한 스트림에 대해 상이한 인코딩 및 암호화 알고리즘이 사용된다.

[0079] 추가적으로 또는 대안적으로, 옵션적으로, 분기는, 입력 데이터(D1)가 동일한 타입의 데이터를 포함하는 경우에도, 인코딩 및 암호화 프로세스를 더 빠르게 만들기 위해 유용하게 구현된다. 이와 관련하여, 인코딩되고 암호화된 데이터(E2)는, 옵션적으로, 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 분기를 구현하기 위해, 입력 데이터(D1)가 어떻게 분할되는지를 나타내는 정보를 포함한다.

[0080] 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위한 시드 값과 조합하여 적어도 하나의 키를 반복적으로 사용하도록 동작가능하다. 한 예에서, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위한 적어도 하나의 키에 시드 값을 전치부가하도록(prepend) 동작가능하다. 다른 예에서, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위한 적어도 하나의 키에, 시드 값을 부가하도록(append) 동작가능하다.

[0081] 대안적으로, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 적어도 하나의 키를 사용하도록 동작가능하다. 이러한 경우에, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 시드 값을 단독으로 사용하도록 동작가능하다. 다시 말하면, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷은 적어도 하나의 키를 단독으로 사용하여 암호화된다.

[0082] 또한, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 동작가능하다.

[0083] 또한, 본 개시의 한 실시형태에서 채용되는 하나의 기술적 구현 모델에서는, 시드 값의 생성을 가능하게 하기 위해, 즉, 시드 값을 생성하기 위한 프로그램 루틴 또는 함수를 호출하기 위해, 인터셉트 기능성이 인코더(110)에 기록된다.

[0084] 본 개시의 하나의 실시형태에서, 시드 값을 생성하기 위해 사용되는 정보는 디코더(120)로 정의되거나 또는 전달되고, 그 결과 암호화 프로세스는 후속하는 암호해제 동안 역으로 될 수 있다. 이와 관련하여, 인코더(110)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 인코딩되고 암호화된 데이터(E2)에 포함시키도록 동작가능하다.

[0085] 데이터 블록 및/또는 데이터 패킷 사이에서 시드 값을 변경하는 것은, 암호화 프로세스의 효율성을 향상시킨다.

[0086] 시드 값은 입력 데이터(D1)에 존재하는 잠재적으로 거의 모든 종류의 정보로부터 계산될 수도 있다. 그러나, 디코더(120)에서의 후속하는 암호해제 동안, 자신의 생성이 인코딩 및 암호화 프로세스의 해석을 필요로 할 시드 값을 인코딩 및 암호화 프로세스의 통합이 생성하지 않을 것이기 때문에, 실질적으로 인코딩되고 암호화된 데이터(E2)를 제공하는 프로세싱된 데이터로부터는 시드 값이 유용하게 계산될 수 없다는 것이 인식될 것이다. 다시 말하면, 시드 값은, 인코딩되고 암호화된 데이터(E2) 단독으로부터는 직접적으로 도출될 수 없는 인코딩 프로세스에 의해 생성되는 다양한 순시 정보(instantaneous information)로부터 유용하게 계산된다. 옵션적으로, 시드 값은, 변하는 파라미터의 도움을 받는 프로세스에 의해 요구된다.

[0087] 하나의 구현예에서, 시드 값은, 예를 들면, 체크썸 또는 해시 함수를 사용하는 것에 의해 인코딩 프로세스가 수행되기 이전에 계산된다. 이것은 잠재적으로 관련된 암호해제 프로세스를 약간 더 간단하게 만들지만, 그러나 종래 기술의 방법과 비교하여 여전히 향상되게 만든다. 한 예에서, 체크썸 또는 해시 함수는 입력 데이터(D1)의 주어진 데이터 블록 및/또는 데이터 패킷의 적어도 한 부분에 대해 계산된다. 시드 값을 역 엔지니어링(reverse engineering)하는 것을 방지하기 위해, 시드 값은 양방향의 초기 값에 기초하여 생성될 수 없다는 것이 인식될 것이다. 또한, 확률 계산을 사용하는 것을 방지하기 위해, 시드 값은 예측에 의해서도 또한 생성될 수 없다. 유익하게는, 시드 값은 일방향 해싱 알고리즘을 사용하여 계산된다.

[0088] 다른 구현예에서, 시드 값은, 고급 암호 표준(Advanced Encryption Standard; AES) 암호화 알고리즘의 암호 블록 체인화(Cipher-Block Chaining; CBC) 모드를 사용하는 것에 의해 암호화 프로세스가 수행되기 이전에 계산된다. 이러한 경우에, 이전의 데이터 블록 및/또는 패킷의 암호화된 출력, 즉 비문은, 암호화되고 있는 주어진 데이터 블록 및/또는 데이터 패킷, 즉 평문과 조합된다. 이것은, AES 암호화 알고리즘의 CBC 모드가 다른 점에서는 보통처럼 작용하고 있지만, 인코딩 프로세스에 의해 생성되는 시드 값이 암호화된 출력, 즉 인코딩되고 암호화된 데이터(E2)에 삽입된다는 것을 의미한다. 암호화 프로세스는 또한, 스트림 암호, 즉 대칭 키 암호를 사용하는 것에 의해 발생할 수 있는데, 이 경우 평문 디지트(digit)는 의사 랜덤 암호 디지트 스트림, 즉 "키스트림"과 결합된다. 이러한 경우에, 데이터 블록 및/또는 데이터 패킷은 하나 이상의 데이터 스트림에 의해 대체된다.

[0089] 본 개시의 실시형태에서, 이러한 씨드 기반의 암호화를 위해 사용되는 및/또는 송신되는 시드 값이 계산될 수 있는 여러 개의 옵션적인 방식이 존재한다. 이들 옵션은, 예를 들면, 인코딩되고 암호화된 데이터(E2)의 주어진 사용 시나리오 및/또는 목표에, 및/또는 암호화 프로세스를 위해 채용되는 암호화 알고리즘에 의존한다.

[0090] 본 개시의 대안적인 실시형태에서, 시드 값을 생성하기 위해 사용되는 정보가 달리 디코더(120)로 정의되거나 또는 전달되지 않는 경우, 시드 값이 어떻게 생성되는지에 관해 적어도 부분적으로 나타내는 정보가, 옵션적으로, 인코더(110)로부터 디코더(120)로 송신된다. 이것은, 시드 값이 입력 데이터(D1)에 관련되지 않는 또는 랜덤하게 생성되는 경우에 특히 유용하다. 그러나, 보안 이유 때문에, 이러한 경우의 시드 값은 절대 송신되지 않는 것이 바람직하다.

[0091] 또한, 옵션적으로, 인코더(110)는 데이터베이스(도 1에서 도시되지 않음)에 저장하기 위해 인코딩되고 암호화된 데이터(E2)를 데이터 서버 및/또는 데이터 스토리지(도 1에서 도시되지 않음)로 전달하도록 동작가능하다. 데이터 서버 및/또는 데이터 스토리지는, 인코딩되고 암호화된 데이터(E2)를 후속하여 암호해제하고 디코딩하기 위해, 인코더(110)와 유용하게 호환가능한 디코더(120)가 액세스할 수 있도록 배치된다.

[0092] 추가적으로, 옵션적으로, 인코더(110)는, 적어도 하나의 키 및/또는 초기화 벡터(IV) 및/또는 시드 값을 생성하기 위해 채영되는 적어도 하나의 알고리즘을 나타내는 정보를, 데이터베이스에 저장하기 위해, 데이터 서버 및/또는 데이터 스토리지로 전달하도록 동작가능하다.

[0093] 몇몇 예에서, 디코더(120)는, 옵션적으로, 데이터 서버 및/또는 데이터 스토리지로부터 인코딩되고 암호화된 데이터(E2)에 액세스하도록 동작가능하다. 추가적으로, 옵션적으로, 디코더(120)는, 적어도 하나의 키 및/또는 IV 및/또는 시드 값을 생성하기 위해 채용되는 적어도 하나의 알고리즘을, 데이터 서버 및/또는 다른 데이터 서버 및/또는 데이터 스토리지로부터 액세스하도록 동작가능하다.

[0094] 대안적인 예에서, 인코더(110)는, 옵션적으로, 통신 네트워크를 통해 또는 직접 연결을 통해, 인코딩되고 암호화된 데이터(E2)를 디코더(120)로 스트리밍하도록 동작가능하다. 또한, 하드웨어 기반의 또는 소프트웨어 기반의 인코더를 갖춘 디바이스는 또한, 하드웨어 기반의 또는 소프트웨어 기반의 디코더를 갖춘 다른 디바이스와 직접적으로 통신할 수 있다는 것을 유의해야 한다.

[0095] 여전히 다른 대안적인 예에서, 디코더(120)는, 옵션적으로, 하드 드라이브 및 솔리드 스테이트 드라이브(Solid-

State Drive; SSD)와 같은 비일시적(즉 일시적이지 않은) 컴퓨터 판독가능 저장 매체로부터 인코딩되고 암호화된 데이터(E2)를 검색하도록(retrieve) 구현된다.

[0096] 또한, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)의 후속하는 암호해제 및 디코딩에서 사용하기 위한 적어도 하나의 키의, 인코더(110)로부터 디코더(120)로의 전달을 조정하도록 동작가능하다. 옵션적으로, 적어도 하나의 키는 인코더(110)로부터 디코더(120)로, 그 각각의 유저 사이에서 수동으로 전달된다. 대안적으로, 옵션적으로, 적어도 하나의 키는 인코더(110)로부터 디코더(120)로 암호화된 이메일을 통해, 예를 들면, 예컨대 프리티 굳 프라이버시(PGP), GNU 프라이버시 가드(GNU Privacy Guard; GnuPG), 또는 유사한 것을 사용하여 암호화되는 이메일을 통해, 전달된다. 여전히 대안적으로, 옵션적으로, 적어도 하나의 키는 인코더(110)로부터 디코더(120)로 암호화된 통신 연결을 통해 전달된다. 옵션적으로, 암호화된 통신 연결은, 보안 소켓 레이어(SSL)/전송 레이어 보안(TLS) 프로토콜을 통해 구현된다.

[0097] 디코더(120)는, 대응하는 디코딩된 데이터(D3)를 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 프로세싱하기 위한 데이터 프로세싱 장치를 포함한다. 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 하기에 상세히 설명되는 바와 같이 프로그램 명령어를 실행하도록 동작가능한 적어도 하나의 RISC 프로세서를 채용하는 것에 의해 구현되고; 이러한 RISC 프로세서는, 상대적으로 더 간단한 사슬연결된 연산을 아주 빠른 속도로 수행할 수 있고, 스트리밍 포맷으로 제공되는 데이터를, 예를 들면, 실시간으로 인코딩하고 디코딩하는 데 적합하다.

[0098] 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 1차원 데이터, 인코딩되고 암호화된 다차원 데이터, 인코딩되고 암호화된 텍스트 데이터, 인코딩되고 암호화된 이진 데이터, 인코딩되고 암호화된 센서 데이터, 인코딩되고 암호화된 오디오 데이터, 인코딩되고 암호화된 이미지 데이터, 인코딩되고 암호화된 비디오 데이터(이들로 제한되지는 않음) 중 적어도 하나의 형태로 제공되는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 동작가능하다.

[0099] 앞서 설명된 바와 같이, 디코더(120)의 데이터 프로세싱 장치는 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 동작 중에 제공받는다.

[0100] 디코더(120)의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 적어도 하나의 키를 사용하여 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하도록 동작가능하다. 그 다음, 디코더(120)의 데이터 프로세싱 장치는, 디코딩된 데이터(D3)에 포함시키기 위한 제1 디코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩하도록 동작가능하다.

[0101] 앞서 설명된 바와 같이, 인코딩되고 암호화된 데이터(E2), 유용하게도, 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해 인코더(110)에서 채용되는 적어도 하나의 알고리즘을 나타내는 정보를 포함한다. 이 정보를 사용하여, 디코더(120)의 데이터 프로세싱 장치는, 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제함에 있어서 사용하기 위한 제1 시드 값을 생성하도록 동작가능하다. 그 다음, 디코더(120)의 데이터 프로세싱 장치는, 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩하도록 동작가능하다.

[0102] 계속해서, 디코더(120)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)의 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷이 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하고 디코딩함에 있어서 사용하기 위한 다음 번 시드 값을 순차 반복적 방식으로 생성하도록 동작가능하다.

[0103] 이 방식에서, 옵션적으로, 인코딩되고 암호화된 데이터(E2)의 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷은 하나씩 차례로 단계적으로 디코딩된 데이터(D3)로 암호해제 및 디코딩된다.

[0104] 또한, 옵션적으로, 디코딩된 데이터(D3)를 생성하기 위해, 디코더(120)의 데이터 프로세싱 장치는 인코더(110)의 데이터 프로세싱 장치에 의해 수행되는 인코딩 및 암호화 프로세스의 역(reverse)을 수행하도록 동작가능하다. 이와 관련하여, 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 엔트로피 수정 디코딩, 델타 디코딩, ODelta 디코딩, 1u 또는 8u 범위 디코딩, 런 렝쓰 디코딩, 스플릿 런 렝쓰 디코딩, 및/또는 보간 디코딩 중 적어도 하나를 채용하는 것에 의해 인코딩된 데이터 블록 및/또는 데이터 패킷에 대해 추가적인 디코딩 프로세스

를 수행하도록 동작가능하다.

[0105] 또한, 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 연관된 시드 값을 사용하여 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 암호해제 및 디코딩의 복수의 동시적 시퀀스로 분기하는 것에 의해 대응하는 디코딩된 데이터(D3)를 순차 반복적 방식으로 생성하기 위해 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하도록 동작가능하다. 옵션적으로, 이러한 분기를 구현하기 위해, 인코딩되고 암호화된 데이터(E2)는, 예를 들면, 입력 데이터(D1)에서 존재하는 데이터의 각각의 상이한 타입에 대해, 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 상이한 스트림을 포함한다.

[0106] 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위한 시드 값과 조합하여 적어도 하나의 키를 반복적으로 사용하도록 동작가능하다. 한 예에서, 디코더(120)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위한 적어도 하나의 키에, 시드 값을 전치부가하도록 동작가능하다. 다른 예에서, 디코더(120)의 데이터 프로세싱 장치는, 옵션적으로, 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위한 적어도 하나의 키에, 시드 값을 부가하도록 동작가능하다.

[0107] 대안적으로, 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 적어도 하나의 키를 단독으로 사용하도록 동작가능하다. 이러한 경우에서, 디코더(120)의 데이터 프로세싱 장치는, 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 시드 값을 단독으로 사용하도록 동작가능하다.

[0108] 또한, 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용하도록 동작가능하다.

[0109] 또한, 옵션적으로, 인코딩 동안, 주어진 데이터 블록 및/또는 데이터 패킷은, 자신의 후속하는 데이터 블록 및/또는 데이터 패킷을 암호화함에 있어서 사용하기 위한 시드 값을 생성하기 위해, 프로세싱된다. 결과적으로, 시드 값은 주어진 데이터 블록 및/또는 데이터 패킷의 컨텐츠에 기초한다. 따라서, 암호해제 및 디코딩 동안, 주어진 인코딩되고 암호화된 데이터 및/또는 데이터 패킷은, 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 정확하게 암호해제하고 디코딩하는 것을 가능하게 하기 위해, 정확하게 암호해제되고 디코딩될 필요가 있다. 이 방식에서, 인코딩되고 암호화된 데이터(E2)로부터의 디코딩된 데이터(D3)의 생성은, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 암호해제 및 디코딩을 하나씩 차례로 단계적으로 수행하는 것을 필요로 한다.

[0110] 인코딩 및 암호화 프로세스의 상기 언급된 통합은, 이렇게 달성되는 암호화를 깨기 위해 무단 침입 공격자가 필요로 할 컴퓨팅 리소스의 양을 증가시킨다. 결과적으로, 암호화를 깨뜨리려는 시도에 필요한 시간은 암호해독자에게 신규의 도전과제를 제시한다.

[0111] 기술적 관점에서, 예를 들면, 압축을 통해 암호화 이전에 입력 데이터(D1)의 복수의 데이터 블록 및/또는 데이터 패킷을 인코딩하는 것은 비용 효율적인데, 그 이유는, 이러한 경우, 인코딩되고 암호화된 데이터(E2)의 엔트로피 및 데이터 사이즈가, 입력 데이터(D1)가 압축 이전에 암호화된 경우보다 더 작기 때문이다. 암호화 알고리즘은 통상적으로 인코딩되고 암호화된 데이터(E2)에서 최대 데이터 엔트로피를 생성하는 경향이 있는데, 이것은 수학적으로, 이론적으로 가능한 바와 같이, 인코딩되고 암호화된 데이터(E2)를 해독하기(deciphering) 위한 많은 선택 여지가 존재한다는 것을 의미한다. 압축은 또한, 옵션적으로, 입력 데이터(D1)의 개개의 데이터 블록 및/또는 데이터 패킷 대신, 전체 입력 데이터(D1)에 종속된다는 것이 인식될 것이다. 이러한 경우, 압축, 즉 인코딩에 의해 생성되는 시드 값을 보안적 방식으로, 예를 들면 암호화된 데이터로서 일시적으로 저장하기 위한 메커니즘이 채용된다.

[0112] 도 1은, 본원의 청구범위를 부당하게 제한하지 않아야 하는 예에 불과하다. 코덱(130)에 대한 특정 목적지는 예로서 제공되며, 특정한 수, 타입, 배치의 인코더 및 디코더로 코덱(130)을 제한하는 것으로 해석되지 않아야 한다는 것이 또는 이해되어야 한다. 기술 분야의 숙련된 자는, 본 개시의 실시형태의 많은 변형예, 대안예, 및 수정예를 인식할 것이다.

[0113] 옵션적으로, 코덱(130)은 단일의 디바이스 내에서 구현된다. 대안적으로, 옵션적으로, 코덱(130)은 다수의 디바이스 사이에서 효과적으로 구현된다. 옵션적으로, 코덱(130)은, 예를 들면, 하나 이상의 주문형 반도체(application-specific integrated circuit; ASIC)의 사용을 통해, 주문 설계(custom-design) 디지털 하드웨어로서 구현된다. 대안적으로, 또는 추가적으로, 코덱은 컴퓨팅 하드웨어 상에서 실행가능한 컴퓨터 소프트웨어

명령어로 구현된다.

[0114] 코덱(130)은 데이터 코덱, 오디오 코덱, 이미지 코덱 및/또는 비디오 코덱(이들로 제한되지는 않음) 중 적어도 하나로서 구현될 수 있다.

[0115] 또한, 코덱(130)은, 데이터 전송에 필요로 되는 네트워크 대역폭을 상당히 절약하면서, 그리고 데이터 전송을 위한 암호화된 통신 연결, 예컨대 SSL/TLS을 필요로 하지 않으면서, 전송측과 수신측 사이에 보안 통신을 제공하도록 구현될 수 있다. 한 예에서, 코덱(130)은, 요구-응답 타입의 통신에 기초한 그러한 시스템, 예컨대 데이터 전송을 위한 웹 브라우저 및 월드 와이드 웹(World Wide Web; www) 서버에서 사용되는 하이퍼텍스트 전송 프로토콜(HyperText Transfer Protocol; HTTP)에서 구현될 수도 있다.

[0116] 오늘날 암호화되는 데이터는, 미래의 "무차별 대입 공격(brute force attack)" 기술을 사용하는 것에 의해 깨지거나 암호해제될 가능성이 있지만, 미래의 암호화 알고리즘은, 상응하게, 현재의 암호화 알고리즘보다 더 강력한 암호화 키를 생성할 것이고, 따라서 여전히 데이터의 강력한 암호화를 보장할 것이다는 것이 가정된다.

[0117] "무차별 대입 공격" 기술 외에, "biclique 공격", "관련 키 공격(related-key attack)", "패딩 오라클 공격(padding oracle attack)", "길이 확장 공격(length extension attack)" 기술 및 등등과 같은 다른 널리 공지된 공격 기술이 존재하지만, 이들 기술은 본질적으로 인코더(110)에 의해 수행되는 암호화를 깨지 못한다.

[0118] 단지 예시 목적을 위해, 다음에서는, 암호화 프로세스의 기술적 예가 인코더(110)에서 실행되는 것으로 제공된다. 이 예에서는, CBC 모드의 대칭 AES 암호화 알고리즘 및 다음의 단계를 따라 확장된 암호화 키를 갖는 시드 값을 사용하는 것에 의해, 암호화되지 않은 평문 데이터 스트림을 암호화하기 위한 하나의 일반적으로 효율적인 모델이 제시된다.

[0119] 1. 두 개의 암호화 키, 즉 키1 및 키2를 획득하거나 생성한다;

[0120] 2. AES CBC에 대한 암호 랜덤 초기화 벡터(IV)를 생성한다;

[0121] 3. 키1 및 IV 또는 키1 및 솔트(Salt)를 갖는 AES CBC 함수를 사용하여 평문 바이트(즉, 인코딩된 데이터 블록 및/또는 데이터 패킷)를 비문 바이트(즉, 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷)으로 암호화한다;

[0122] 4. IV 및 비문 바이트를 병합한다;

[0123] 5. 키2 및 비문을 갖는 HMAC 함수를 사용하여 메시지 인증 코드(Message Authentication Code; MAC) 바이트를 생성한다; 그리고

[0124] 6. MAC 및 비문 바이트를 데이터 스트림, 즉 인코딩되고 암호화된 데이터(E2)로 기록한다.

[0125] 또한, 상기 언급된 알고리즘의 의사 코드는 다음과 같이 표현된다.

[0126] Key1 = KeyStretch(GetKey())

[0127] Key2 = KeyStretch(GetKey())

[0128] IV = Random()

[0129] Ciphertext = IV + AES(Key1 + Salt, IV, Plaintext)

[0130] MAC = HMAC(Key2, Ciphertext)

[0131] DATA = MAC + Ciphertext

[0132] 상기 예에서, "키 스트레칭(key stretching)"을 사용하여 두 개의 강화된 키가 생성되었다. "키 스트레칭" 기술은 통상적으로, 일방향 다이제스트 알고리즘, 즉 해싱 알고리즘을 통해 암호화용 패스워드를 수천 번 실행시키는 것에 의해 구현된다. 이것은, 패스워드를, 공격, 즉 키 관련 공격으로부터 보호하는 충분한 치환(permutation)을 생성한다.

[0133] 그 다음, CBC 모드에 대해, 대응하는 랜덤 초기화 벡터(IV) 바이트가 생성된다. 그 다음, 이들 IV 바이트는, 암호화될 제1 인코딩된 데이터 블록 및/또는 데이터 패킷으로 스크램블링 및 혼합된다. 그 다음, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷은, 다수의 확장된 키 및 IV 바이트를 가지고 CBC 모드의 AES 암호화 알고리즘을 사용하여 암호화된다.

[0134] 제1 인코딩된 데이터 블록 및/또는 데이터 패킷에 대해 IV 바이트를 사용하는 것은 암호화의 보호의 정도를 향상시키는 목적에 대해 특히 유익하며, 따라서, 예를 들면, 입력 데이터(D1)가 많은 중복 데이터를 포함하는 경우에 획득된다. 결과적으로, 인코딩되고 암호화된 데이터(E2)의 각각의 인코딩되고 암호화된 데이터 및/또는 데이터 패킷이 처음부터 끝까지 깨지기 전에는, 무단 침입하는 공격자는 정보의 전체 시퀀스, 즉 입력 데이터(D1)를 암호해제할 수 없다.

[0135] 다음으로, 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷은, 인코딩 프로세스에 의해 생성되는 다수의 확장된 키 및 시드 값을 가지고 CBC 모드의 대칭 AES 암호화 알고리즘을 사용하여 암호화된다.

[0136] 마지막으로, 메시지 인증 코드(MAC) 바이트가 비문에, 즉 인코딩되고 암호화된 데이터(E2)에 삽입된다. 이것은, 입력 데이터(D1)에서 어쩌면 발생하는 중복 평문에 의해 야기되는 어쩌면 동일한 비문을 방지하고, 또한, 예를 들면, "패딩 오라클 공격" 기술을 통해, 암호화가 깨지는 것을 방지한다. 이것은 또한, 인코딩되고 암호화된 데이터(E2)의 무결성이 완전하다는 것을 보장한다.

[0137] 비록 도면에서 설명되는 실시형태가 CBC, 즉 암호 블록 체인화 모드를 사용하여 표시되지만, 본 개시의 실시형태는 또한 스트림 암호를 사용하는 것에 구현될 수 있다는 것이 인식될 것인데, 이 경우 데이터 블록 및/또는 데이터 패킷은 하나 이상의 데이터 스트림에 의해 대체된다.

[0138] 이제 도 2를 참조하면, 본 개시의 다른 실시형태에 따른, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해, 복수의 데이터 블록 및/또는 데이터 패킷을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하는 제1 통합 방법의 단계를 묘사하는 플로우차트가 제공된다. 방법은, 예를 들면, 상기 언급된 바와 같이, 하드웨어, 소프트웨어, 또는 이들의 조합으로 구현될 수 있는 단계의 시퀀스를 나타내는 논리적 흐름도에서 단계의 콜렉션으로 묘사된다.

[0139] 단지 예시 목적을 위해, 다음에, 방법은 도 1에서 묘사되는 인코더(110)를 참조로 예시될 것이다.

[0140] 단계 202에서, 인코더(110)의 데이터 프로세싱 장치는 복수의 데이터 블록 및/또는 데이터 패킷 중 제1 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0141] 다음에, 단계 204에서, 인코더(110)의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해, 제1 데이터 블록 및/또는 데이터 패킷을 인코딩한다.

[0142] 옵션적으로, 단계 204에서, 인코더(110)의 데이터 프로세싱 장치는, 복수의 데이터 블록 및/또는 데이터 패킷 중 다음 번 데이터 블록 및/또는 데이터 패킷의 암호화에서 사용하기 위한 제1 시드 값을 생성하기 위해 제1 데이터 블록 및/또는 데이터 패킷을 프로세싱한다. 시드 값은, 이하, "솔트"로 상호교환적으로 칭해진다.

[0143] 계속해서, 단계 206에서, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 적어도 하나의 키를 사용하여 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화한다.

[0144] 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는 인코딩되고 암호화된 데이터(E2)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 제공받는다. 대안적으로, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 적절한 키 생성 알고리즘을 사용하여 적어도 하나의 키를 생성한다.

[0145] 추가적으로, 옵션적으로, 인코더(110)의 데이터 프로세싱 장치는, 단계 206에서 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용한다.

[0146] 다음에, 단계 208에서, 인코더(110)의 데이터 프로세싱 장치는 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을, 인코딩되고 암호화된 데이터(E2)에 기록 또는 송신한다.

[0147] 단계 210에서, 인코더(110)의 데이터 프로세싱 장치는, 복수의 데이터 블록 및/또는 데이터 패킷 중 다음 번 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0148] 다음에, 단계 212에서, 인코더(110)의 데이터 프로세싱 장치는, 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 다음 번 데이터 블록 및/또는 데이터 패킷을 인코딩한다.

[0149] 옵션적으로, 단계 212에서, 인코더(110)의 데이터 프로세싱 장치는, 복수의 데이터 블록 및/또는 데이터 패킷 중 후속하는 데이터 블록 및/또는 데이터 패킷의 암호화에서 사용하기 위한 다음 번 시드 값을 생성하기 위해 다음 번 데이터 블록 및/또는 데이터 패킷을 프로세싱한다.

[0150] 계속해서, 단계 214에서, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 적어도 하나의 키와 조합하여 단계 204에서 생성되는 제1 시드 값을 사용하여 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화한다.

[0151] 이 목적을 위해, 제1 시드 값 및 적어도 하나의 키는 다양한 방식으로 병합될 수 있다. 예로서, 적어도 하나의 키는 제1 시드 값을 적어도 하나의 키에 전치부가하는 또는 부가하는 것에 의해 솔팅된다(salted).

[0152] 다음에, 단계 216에서, 인코더(110)의 데이터 프로세싱 장치는 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을, 인코딩되고 암호화된 데이터(E2)에 기록 또는 송신한다.

[0153] 마찬가지로, 단계 218에서, 인코더(110)의 데이터 프로세싱 장치는 복수의 데이터 블록 및/또는 데이터 패킷 중 후속하는 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0154] 다음에, 단계 220에서, 인코더(110)의 데이터 프로세싱 장치는, 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해, 후속하는 데이터 블록 및/또는 데이터 패킷을 인코딩한다.

[0155] 옵션적으로, 단계 220에서, 인코더(110)의 데이터 프로세싱 장치는, 복수의 데이터 블록 및/또는 데이터 패킷 중 더 후속하는(yet subsequent) 데이터 블록 및/또는 데이터 패킷의 암호화에서 사용하기 위한 후속하는 시드 값(도 2에서는 도시되지 않음)을 생성하기 위해 후속하는 데이터 블록 및/또는 데이터 패킷을 프로세싱한다.

[0156] 계속해서, 단계 222에서, 인코더(110)의 데이터 프로세싱 장치는, 인코딩되고 암호화된 데이터(E2)에 포함시키기 위한 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 적어도 하나의 키와 조합하여 단계 212에서 생성되는 다음 번 시드 값을 사용하여 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화한다. 이 목적을 위해, 다음 번 시드 값 및 적어도 하나의 키는, 예를 들면, 다음 번 시드 값을 적어도 하나의 키에 전치부가하거나 또는 부가하는 것에 의해 병합될 수 있다.

[0157] 다음에, 단계 224에서, 인코더(110)의 데이터 프로세싱 장치는, 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을, 인코딩되고 암호화된 데이터(E2)에 기록 또는 송신한다.

[0158] 단계 218 내지 224는, 입력 데이터(D1)의 복수의 데이터 블록 및/또는 데이터 패킷이 인코딩되고 암호화된 데이터(E2)로 인코딩되고 암호화될 때까지, 순차 반복적 방식으로 수행된다.

[0159] 단계 202 내지 224는 단지 예시적인 것이며, 본원의 청구범위의 범주를 벗어나지 않으면서 하나 이상의 단계가 추가되는, 하나 이상의 단계가 제거되는, 또는 하나 이상의 단계가 상이한 순서로 제공되는 다른 대안예도 또한 제공될 수 있다. 대안적인 실시형태에서, 복수의 데이터 블록 및/또는 데이터 패킷의 인코딩은, 그들의 대응하는 인코딩된 데이터 블록 및/또는 데이터 패킷의 암호화가 시작하기 이전에, 수행된다. 다시 말하면, 단계 202, 204, 210, 212, 218 및 220, 즉, 입력 데이터(D1)의 데이터 블록 및/또는 데이터 패킷의 판독 및 인코딩에 관련되는 단계는, 단계 206, 208, 214, 216, 222 및 224, 즉, 인코딩된 데이터 블록 및/또는 데이터 패킷의 암호화 및 인코딩되고 암호화된 데이터(E2)로의 기록에 관한 단계가 수행되기 이전에, 수행된다.

[0160] 도 2에서 도시되는 바와 같이, 단계 206, 214 및 222는, 옵션적으로, 대칭 AES 암호화 알고리즘의 CBC 모드를 사용하여 수행된다. 단계 206은, 옵션적으로, 적어도 하나의 키와 병합되는 랜덤하게 생성된 IV를 사용하여 수행된다. 단계 214 및 222는 그들의 관련된 솔트, 즉 단계 204 및 212에서 각각 생성되는 시드 값을 사용하여 수행된다. 한 예에서, 주어진 데이터 블록 및/또는 데이터 패킷과 관련되는 값 비트의 기수 64 버전(base 64 version)이, 주어진 데이터 블록 및/또는 데이터 패킷의 후속하는 데이터 블록 및/또는 데이터 패킷에 대한 솔트로서 사용된다.

[0161] 도 2에서 묘사되는 방법은, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 IV가 사용되는지 또는 그렇지 않은지의 여부에 무관하게, 그리고 체인식 CBC 모드(chained CBC mode)가 사용되는지 또는 그렇지 않은지의 여부에 무관하게, 다른 암호화 알고리즘을 사용하여 구현될 수 있다는 것이 인식될 것이다.

[0162] 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는, 도 2와 연계하여 설명되는 바와 같은 제1 통합 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다. 컴퓨터 판독가능 명령어는, 옵션적으로, 소프트웨어 애플리케이션 스토어, 예를 들면, "앱 스토어"로부터 컴퓨터화된 디바이스로 다운로드가능하다.

[0163] 도 3은, 본 개시의 실시형태에 따른, 대응하는 디코딩된 데이터(D3)를 생성하기 위해, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 제2 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다. 방법은, 하드웨어, 소프트웨어, 또는 이들의 조합으로 구현될 수 있는 단계의 시퀀스를 나타내는 논리적 흐름도에서 단계의 콜렉션으로 묘사된다.

[0164] 단지 예시 목적을 위해, 다음에, 방법은 도 1에서 묘사되는 디코더(120)를 참조로 예시될 것이다.

[0165] 단계 302에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0166] 다음에, 단계 304에서, 디코더(120)의 데이터 프로세싱 장치는, 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해, 적어도 하나의 키를 사용하여 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제한다.

[0167] 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는 디코딩된 데이터(D3)를 생성함에 있어서 사용하기 위한 적어도 하나의 키를 제공받는다.

[0168] 추가적으로, 옵션적으로, 디코더(120)의 데이터 프로세싱 장치는, 단계 304에서 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위한 적어도 하나의 키와 조합하여 초기화 벡터(IV)를 채용한다.

[0169] 계속해서, 단계 306에서, 디코더(120)의 데이터 프로세싱 장치는, 디코딩된 데이터(D3)에 포함시키기 위한 제1 디코딩된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩한다.

[0170] 옵션적으로, 단계 306에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 암호해제에서 사용하기 위한 제1 시드 값을 생성하기 위해 제1 디코딩된 데이터 블록 및/또는 데이터 패킷을 프로세싱한다.

[0171] 다음에, 단계 308에서, 디코더(120)의 데이터 프로세싱 장치는 제1 디코딩된 데이터 블록 및/또는 데이터 패킷을, 디코딩된 데이터(D3)에 기록 또는 송신한다.

[0172] 단계 310에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0173] 다음에, 단계 312에서, 디코더(120)의 데이터 프로세싱 장치는, 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해 적어도 하나의 키와 조합하여 단계 306에서 생성되는 제1 시드 값을 사용하여 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제한다.

[0174] 이 목적을 위해, 제1 시드 값 및 적어도 하나의 키는 다양한 방식으로 병합될 수 있다. 예로서, 적어도 하나의 키는 제1 시드 값을 적어도 하나의 키에 전치부가하는 또는 부가하는 것에 의해 솔팅된다(salted).

[0175] 계속해서, 단계 314에서, 디코더(120)의 데이터 프로세싱 장치는, 디코딩된 데이터(D3)에 포함시키기 위한 다음 번 디코딩된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩한다.

[0176] 옵션적으로, 단계 314에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 암호해제에서 사용하기 위한 다음 번 시드 값을 생성하기 위해 다음 번 디코딩된 데이터 블록 및/또는 데이터 패킷을 프로세싱한다.

[0177] 다음에, 단계 316에서, 디코더(120)의 데이터 프로세싱 장치는 다음 번 디코딩된 데이터 블록 및/또는 데이터 패킷을, 디코딩된 데이터(D3)에 기록 또는 송신한다.

[0178] 마찬가지로, 단계 318에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 판독 또는 수신한다.

[0179] 다음에, 단계 320에서, 디코더(120)의 데이터 프로세싱 장치는, 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 생성하기 위해, 적어도 하나의 키와 조합하여 단계 314에서 생성되는 다음 번 시드 값을 사용하여 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제한다.

[0180] 이 목적을 위해, 다음 번 시드 값 및 적어도 하나의 키는, 예를 들면, 다음 번 시드 값을 적어도 하나의 키에 전치부가하거나 또는 부가하는 것에 의해 병합될 수 있다.

[0181] 계속해서, 단계 322에서, 디코더(120)의 데이터 프로세싱 장치는, 디코딩된 데이터(D3)에 포함시키기 위한 후속하는 디코딩된 데이터 블록 및/또는 데이터 패킷을 제공하기 위해 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩한다.

[0182] 옵션적으로, 단계 322에서, 디코더(120)의 데이터 프로세싱 장치는, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷 중 더 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷의 암호해제에서 사용하기 위한 후속하는 시드 값(도 3에서 도시되지 않음)을 생성하기 위해 후속하는 디코딩된 데이터 블록 및/또는 데이터 패킷을 프로세싱한다.

[0183] 다음에, 단계 324에서, 디코더(120)의 데이터 프로세싱 장치는 후속하는 디코딩된 데이터 블록 및/또는 데이터 패킷을 디코딩된 데이터(D3)에 기록 또는 송신한다.

[0184] 단계 318 내지 324는, 인코딩되고 암호화된 데이터(E2)의 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷이 디코딩된 데이터(D3)로 암호해제되고 디코딩될 때까지, 순차 반복적 방식으로 수행된다.

[0185] 단계 302 내지 324는 단지 예시적인 것이며, 본원의 청구범위의 범주를 벗어나지 않으면서 하나 이상의 단계가 추가되는, 하나 이상의 단계가 제거되는, 또는 하나 이상의 단계가 상이한 순서로 제공되는 다른 대안예도 또한 제공될 수 있다.

[0186] 도 3에서 도시되는 바와 같이, 단계 304, 312 및 320는, 옵션적으로, 대칭 AES 암호화 알고리즘의 CBC 모드를 사용하여 수행된다. 단계 304는, 옵션적으로, 적어도 하나의 키와 병합되는 랜덤하게 생성된 IV를 사용하여 수행된다. 단계 312 및 320은 그들의 관련된 솔트, 즉 단계 306 및 314에서 각각 생성되는 시드 값을 사용하여 수행된다. 한 예에서, 주어진 디코딩된 데이터 블록 및/또는 데이터 패킷과 관련되는 값 비트의 기수 64 버전이, 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷에 대한 솔트로서 사용된다.

[0187] 도 3에서 묘사되는 방법은, 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 IV가 사용되는지 또는 그렇지 않은지의 여부에 무관하게, 그리고 체인식 CBC 모드가 사용되는지 또는 그렇지 않은지의 여부에 무관하게, 다른 암호해제 알고리즘을 사용하여 구현될 수 있다는 것이 인식될 것이다.

[0188] 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는, 도 3과 연계하여 설명되는 바와 같은 제2 통합 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다. 컴퓨터 판독가능 명령어는, 옵션적으로, 소프트웨어 애플리케이션 스토어, 예를 들면, "앱 스토어"로부터 컴퓨터화된 디바이스로 다운로드가능하다.

[0189] 도 4는, 본 개시의 다른 실시형태에 따른, 대응하는 인코딩되고 암호화된 데이터(E2)를 생성하기 위해, 복수의 데이터 블록 및/또는 데이터 패킷을 포함하는 입력 데이터(D1)를 인코딩하고 암호화하는 제3 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다. 도 2에서 묘사되는 제1 통합 방법의 단계의 설명은, 다르게 언급된 경우를 제외하면, 필요한 부분만 수정한, 도 4에서 묘사되는 제3 통합 방법의 단계에 관련된다. 구체적으로는, 단계 202, 204, 206, 208, 210, 212, 216, 218, 220 및 224의 설명은, 필요한 부분만 수정한, 각각 단계 402, 404, 406, 408, 410, 412, 416, 418, 420 및 424에 관련된다.

[0190] 단계 414는, 다음 번 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 제1 시드 값 값이 단독으로, 즉 적어도 하나의 키 없이 사용되는 점에서, 단계 214와는 상이하다. 마찬가지로, 단계 422는, 후속하는 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 다음 번 시드 값이 단독으로 사용되는 점에서, 단계 222와는 상이하다. 따라서, 제3 통합 방법에서, 인코더(110)의 데이터 프로세싱 장치는, 단계 406에서 제1 인코딩된 데이터 블록 및/또는 데이터 패킷을 암호화하기 위해 적어도 하나의 키를 단독으로 사용하도록 동작가능하다.

[0191] 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는, 도 4와 연계하여 설명되는 바와 같은 제3 통합 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다. 컴퓨터 판독가능 명령어는, 옵션적으로, 소프트웨어 애플리케이션 스토어, 예를 들면, "앱 스토어"로부터 컴퓨터화된 디바이스로 다운로드가능하다.

[0192] 도 5는, 본 개시의 다른 실시형태에 따른, 대응하는 디코딩된 데이터(D3)를 생성하기 위해, 복수의 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 포함하는 인코딩되고 암호화된 데이터(E2)를 암호해제하고 디코딩하는 제4 통합 방법의 단계를 묘사하는 플로우차트의 개략적인 예시이다. 도 3에서 묘사되는 제2 통합 방법의 단계의 설명은, 다르게 언급된 경우를 제외하면, 필요한 부분만 수정한, 도 5에서 묘사되는 제4 통합 방법의 단계에 관련된다. 구체적으로는, 단계 302, 304, 306, 308, 310, 314, 316, 318, 322 및 324의 설명은, 필요한 부분만 수정한, 각각 단계 502, 504, 506, 508, 510, 514, 516, 518, 522 및 524에 관련된다.

[0193] 단계 512는, 다음 번 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 제1 시드 값 값이 단독으로, 즉 적어도 하나의 키 없이 사용되는 점에서, 단계 312와는 상이하다. 마찬가지로, 단계 520는, 후속하는 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 다음 번 시드 값이 단독으로 사용되는 점에서, 단계 320와는 상이하다. 따라서, 제4 통합 방법에서, 디코더(120)의 데이터 프로세싱 장치는, 단계 504에서 제1 인코딩되고 암호화된 데이터 블록 및/또는 데이터 패킷을 암호해제하기 위해 적어도 하나의 키를 단독으로 사용하도록 동작가능하다.

[0194] 본 개시의 실시형태는, 컴퓨터 판독가능 명령어가 저장된 비일시적(즉, 일시적이지 않은) 컴퓨터 판독가능 저장 매체를 포함하는 컴퓨터 프로그램 제품을 제공하는데, 컴퓨터 판독가능 명령어는, 도 5와 연계하여 설명되는 바와 같은 제4 통합 방법을 실행하기 위한 프로세싱 하드웨어를 포함하는 컴퓨터화된 디바이스에 의해 실행가능하다. 컴퓨터 판독가능 명령어는, 옵션적으로, 소프트웨어 애플리케이션 스토어, 예를 들면, "앱 스토어"로부터 컴퓨터화된 디바이스로 다운로드가능하다.

[0195] 상기 언급된 제1 또는 제3 통합 방법은, 인코더로의, 또는 인코더와 관련되는 전처리기(pre-processor)로의 구현에 적합하다; 예를 들면, 상기 언급된 제1 또는 제3 통합 방법은 현존하는 기지의 암호화 방법 및 그 보충 방법(complementary)과 연계하여 사용하기에 적합하다. 마찬가지로, 상기 언급된 제2 및 제4 통합 방법은 디코더로의 또는 디코더와 관련되는 전처리기로의 구현에 적합하다; 예를 들면, 상기 언급된 제2 또는 제4 통합 방법은 현존하는 기지의 암호해제 방법 및 그 보충 방법과 연계하여 사용하기에 적합하다. 상기 언급된 방법은, 소프트웨어에서 및/또는 하드웨어에 내장되는(hardwired) 로직, 예를 들면, 주문형 반도체(ASIC)를 통해 구현될 수 있다. 순수한 소프트웨어 접근방식보다 더 적은 전력을 사용하면서, 암호화를 효율적으로 구현하는, 암호화, 예를 들면 당대의 AES에 대한 전용 마이크로칩을 많은 시스템이 구비한다는 것이 널리 알려져 있다. 상기 언급된 방법은, 예를 들면, 제3자의 공격에 대해, 스파이웨어에 대해 대응하는 저항력을 갖는 암호화를 사용하는 종래 기술의 접근방식과 비교하여, 상당한 전력 및 에너지 절약을 달성하는 것을 가능하게 만든다.

[0196] 본 개시의 실시형태는, 대응하는 암호화 알고리즘을 사용하는 종래 기술의 방법으로 달성되는 보호와 비교하여, 상당한 보호 향상을 가능하게 한다. 본 개시의 실시형태에 따른 방법은, 어떤 암호화 알고리즘이 사용되는지에 무관하게, 임의의 적절한 인코딩 솔루션을 사용하여 구현될 수 있다. 이렇게 함에 있어서, 상기 언급된 방법은 통합된 암호화 알고리즘의 거동을 변경하지는 않는데, 이것은, 통합된 암호화 알고리즘에 의해 제공되는 보호가 손상되지 않는다는 것을 의미한다. 따라서, 본 개시의 실시형태에 따른 방법은 종래 기술의 데이터 압축 및 암호화 알고리즘을, 그들을 협력하는 함수로 함께 통합하는 것에 의해, 더 강화한다.

[0197] 본 개시의 실시형태에 따른 방법은, 특히, 기밀인 또는 기밀 취급되는 지극히 중요한 정보를 보호하기 위한 의료 또는 군사적 목적에서의 효율적인 채용에 적합하다.

[0198] 또한, 상기 언급된 방법은, 일반적으로 널리 알려진 오프 소스 또는 독점적(proprietary) 데이터 압축 소프트웨어 애플리케이션, 예컨대 7-Zip 또는 Win-Zip, 및 등등("7-Zip" 및 "Win-Zip"은 독점적 상표이다)과 연계하여 구현될 수 있다.

[0199] 또한, 인코딩 및 암호화 프로세스의 통합은, 멀티프로세싱에 대한, 또는 여러 프로세스를 병렬 방식으로 실행시키기 위한 효율적인 모델을 제공한다. 통합은, 이용가능한 컴퓨팅 능력에 따른 주어진 중앙 프로세싱 유닛(Central Processing Unit; CPU) 및 주어진 그래픽 프로세싱 유닛(Graphical Processing Unit; GPU)에 대한 최적의 프로세싱 구조의 구현을 가능하게 한다. 따라서, 상기 언급된 방법은, 입력 데이터(D1)의 데이터 블록 및/또는 데이터 패킷이, 인코딩 프로세스가 실행하고 있는 시스템 및/또는 플랫폼의 CPU 및 GPU에 대해 최적인 포맷으로 최적화될 때, 인코딩 프로세스에서의 통합된 암호화 프로세스의 효율적인 스레딩을 가능하게 한다. 암호화 및 암호해제 동안의 상기 언급된 분기는, 각각의 분기에 전용 데이터 프로세싱을 할당하는 것에 의해 병렬 프로세싱 접근방식이 채용되는 것을 가능하게 한다. 고속 데이터 암호화 및 대응하는 데이터의 암호해제를 위한 디지털 어레이 프로세서(digital array processor; DAP)와 같은 컴퓨팅 하드웨어의 사용은 실현 가능하게 된다.

[0200] 상기 언급된 방법은, 아주 빠르지만, 여전히 효율적인 암호화 알고리즘을 사용하는 것을 가능하게 만든다. 이와 관련하여, 상기 언급된 방법은, 암호화 알고리즘 자체의 내부 동작과의 간섭 없이, 암호화 알고리즘을 효율적으로 사용한다. 상기 언급된 방법을 통한 구현에 적합한 암호화 알고리즘의 예는, AES, Twofish, Blowfish, DES(Data Encryption Standard), Triple DES(3-DES), Serpent, IDEA(International Data Encryption Algorithm), MARS, RC6(Rivest Cipher 6), Camellia, CAST-128, Skipjack, XTEA(extended Tiny Encryption Algorithm), 및 등등(이들 예는 등록 상표를 포함한다)을 포함하지만, 그러나 이들로 제한되지는 않는다.

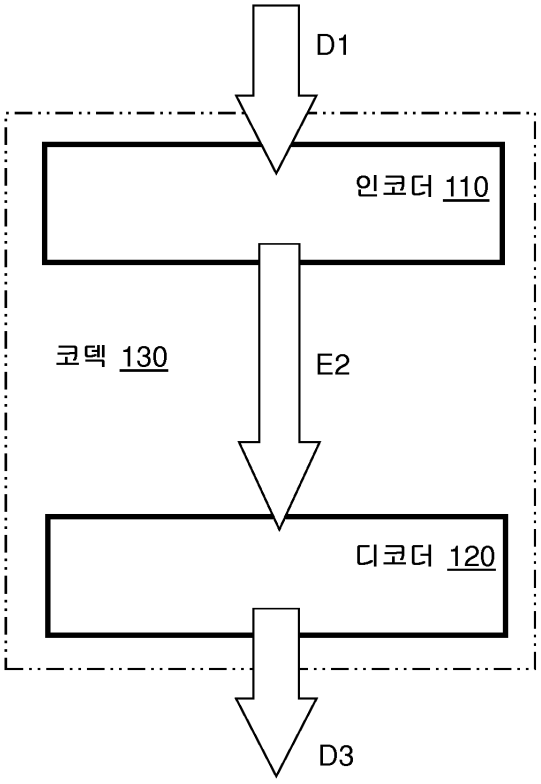
[0201] 또한, 암호화 프로세스를 인코딩 프로세스와 통합하는 추가적인 이점은, 이렇게 생성되는 인코딩되고 암호화된 데이터(E2)가, 예를 들면, 가상 사설 네트워크(Virtual Private Network; VPN) 터널링, 보안 쉘(SSH), 또는 SSL/TLS 프로토콜을 채용하는 보호된 보안 네트워크 연결을 갖는 네트워크를 통해 전송될 필요가 없다는 것이다. 따라서, 상기 언급된 방법은, 예를 들면, 공공 인터넷 네트워크에서 또는 웹서비스 및 클라우드 서비스에서 텍스트, 이진, 오디오, 이미지, 비디오 및 다른 타입의 데이터를 송신하기 위한 유익한 모델을 제공한다.

[0202] 본 개시의 실시형태는, 예를 들면, 스마트 전화, 퍼스널 컴퓨터(Personal Computer; PC), 오디오-비주얼 장치, 카메라, 통신 네트워크, 데이터 저장 디바이스, 감시 시스템, 화상 회의 시스템, 의료 장치, 지진 장치(seismic apparatus), 측량 장치, "블랙 박스" 비행 레코더, 샘플링 기술을 사용하는 디지털 음악 기기와 같은 광범위한 시스템 및 디바이스에서 채용될 수 있지만, 이들로 제한되지는 않는다.

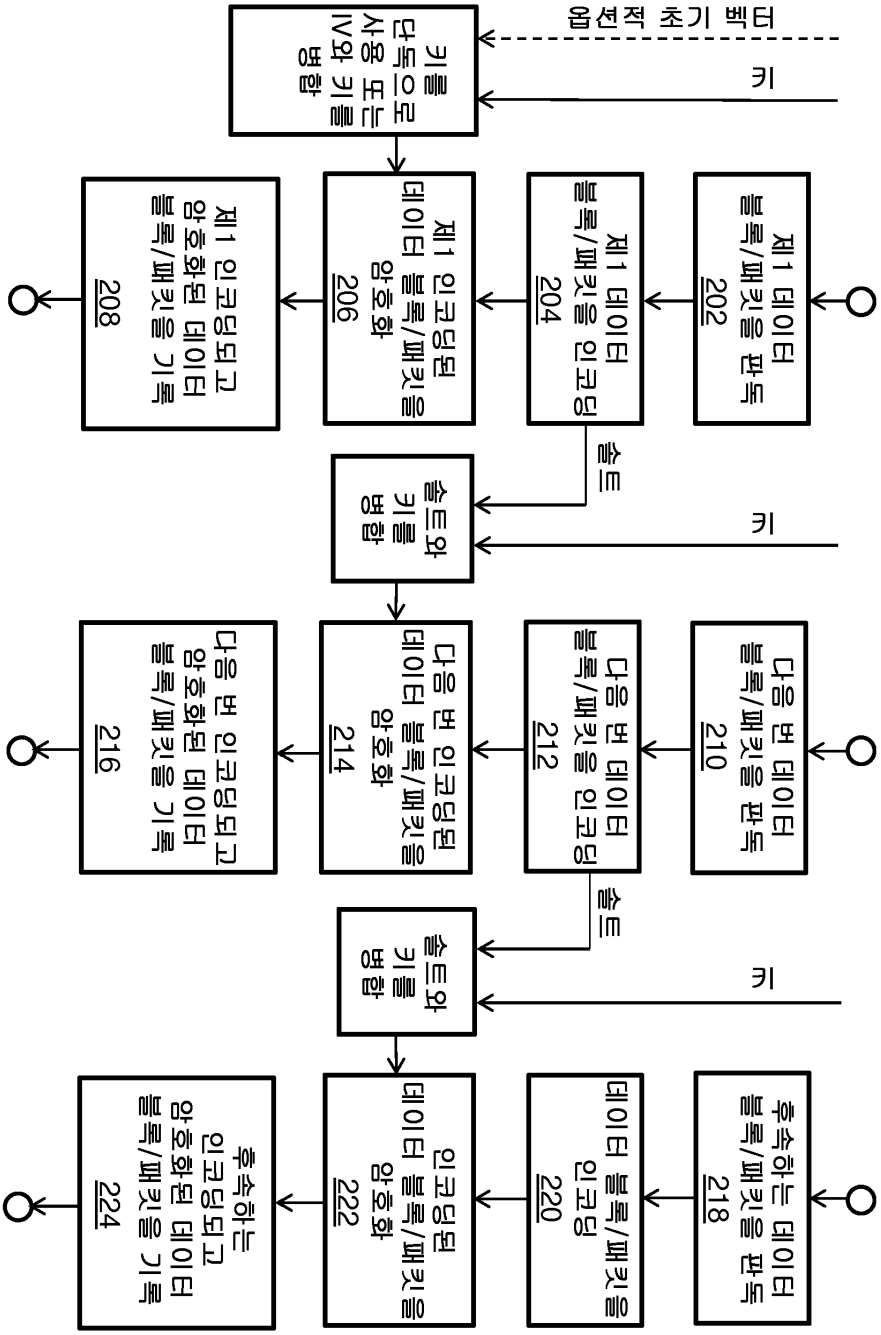
[0203] 첨부의 청구범위에 의해 정의되는 바와 같은 본 발명의 범주를 벗어나지 않으면서, 상기에서 설명되는 본 발명의 실시형태의 수정도 가능하다. 본 발명을 설명하고 청구하기 위해 사용되는 "포함하는(including)", "포함하는(comprising)", "통합하는(incorporating)", "구성되는(consisting of)", "구비한다(have)", "~이다(is)"와 같은 표현은, 비제한적인 방식으로, 즉 명시적으로 설명되지 않는 아이템, 컴포넌트 또는 엘리먼트도 또한 존재하는 것을 허용하는 방식으로 해석되도록 의도된다. 단수에 대한 언급은 또한 복수에 관련되는 것으로 해석되어야 한다. 첨부의 청구범위에서 괄호 안에 포함되는 숫자는 청구범위의 이해를 돕기 위해 의도된 것으로, 이들 청구범위에 의해 청구되는 발명의 대상(subject matter)을 어떤 방식으로든 제한하는 것으로 해석되지 않아야 한다.

## 도면

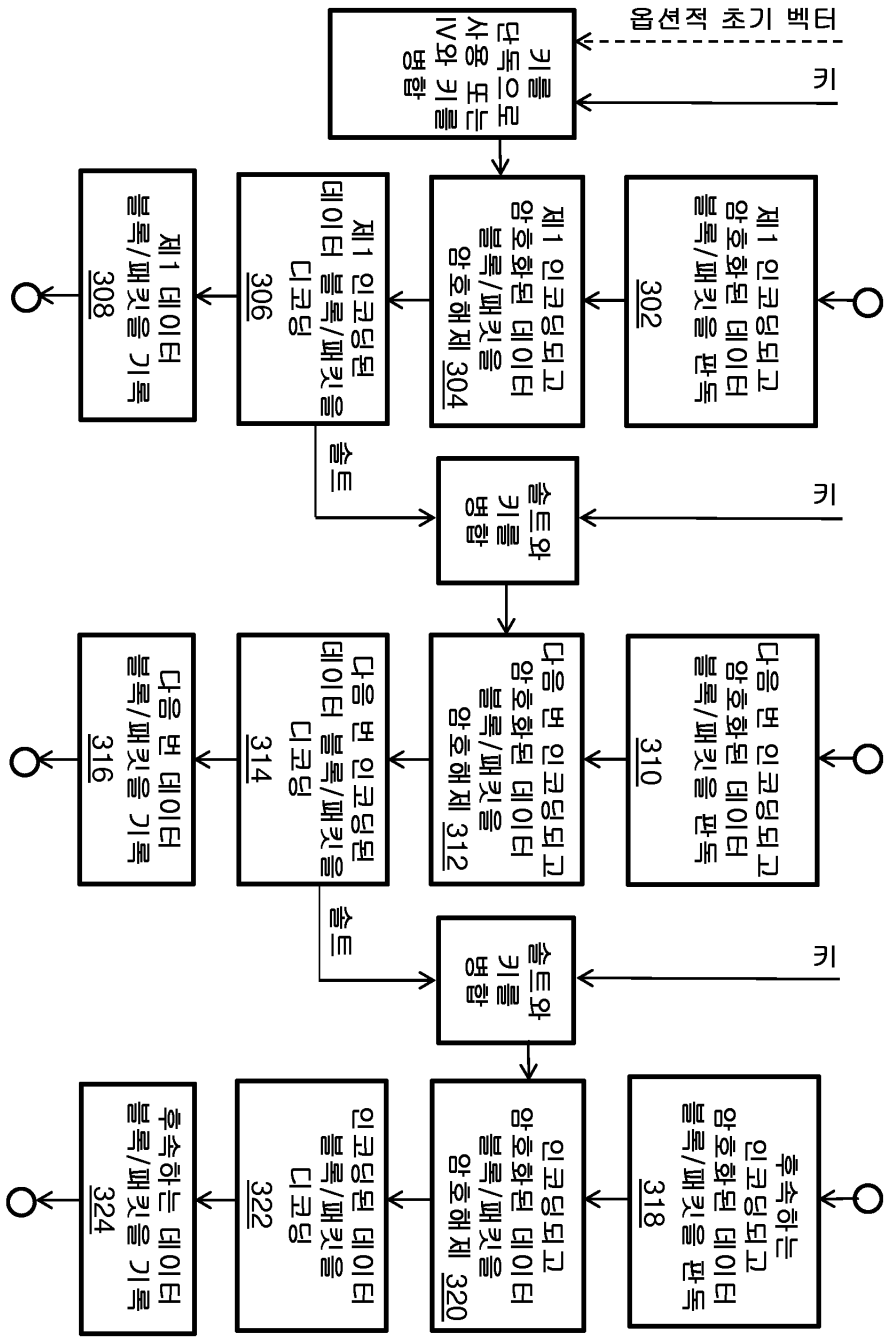
### 도면1



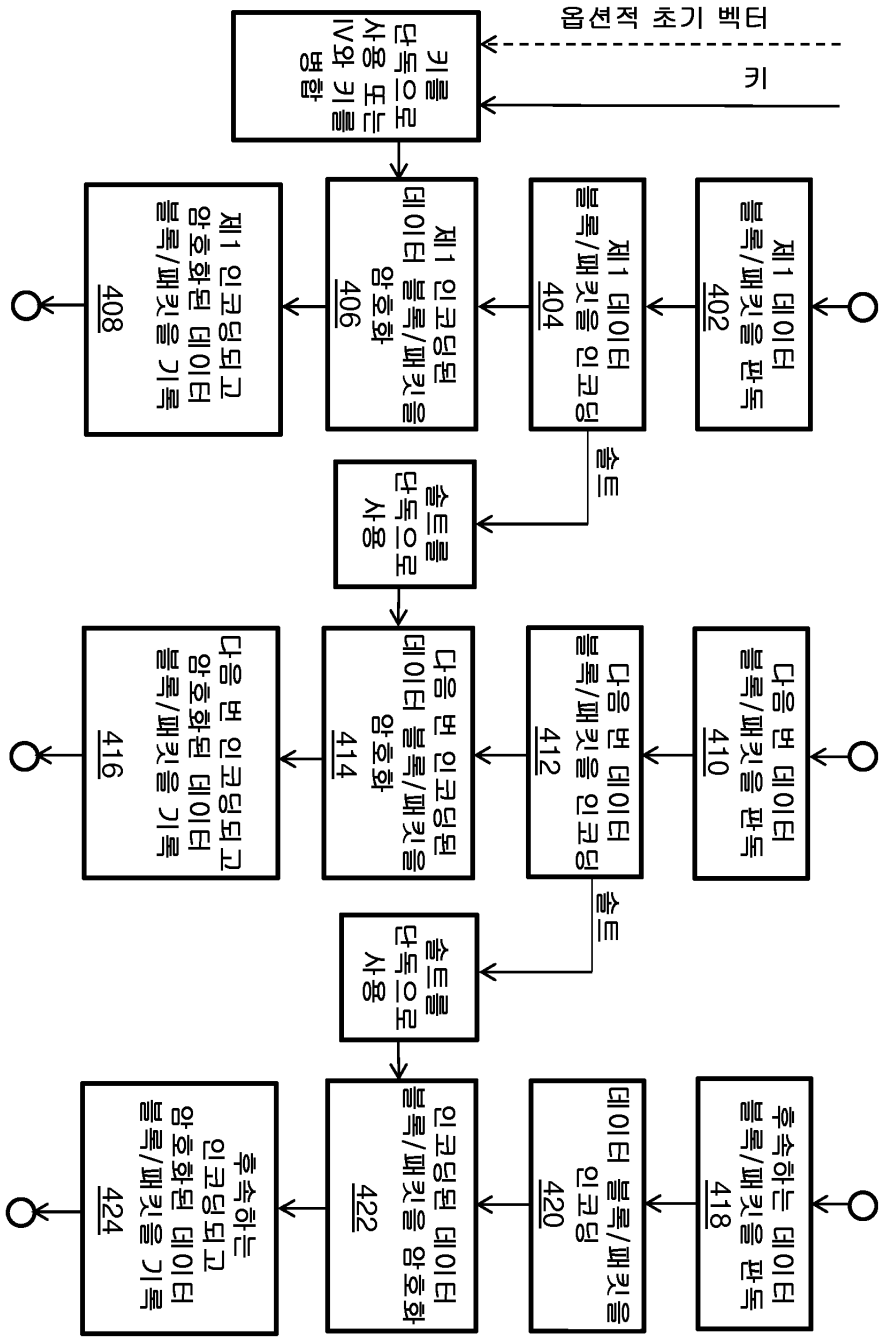
도면2


키를 단독으로 사용 또는 IV와 키를 병합
옵션적 초기 벡터
키
제1 데이터 블록/패킷을 판독
202
제1 데이터 블록/패킷을 인코딩
204
제1 인코딩된 데이터 블록/패킷을 암호화
206
제1 인코딩되고 암호화된 데이터 블록/패킷을 기록
208
솔트
솔트와 키를 병합
키
다음 번 데이터 블록/패킷을 판독
210
다음 번 데이터 블록/패킷을 인코딩
212
다음 번 인코딩된 데이터 블록/패킷을 암호화
214
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 기록
216
솔트
솔트와 키를 병합
키
후속하는 데이터 블록/패킷을 판독
218
데이터 블록/패킷을 인코딩
220
인코딩된 데이터 블록/패킷을 암호화
222
후속하는 인코딩되고 암호화된 데이터 블록/패킷을 기록
224

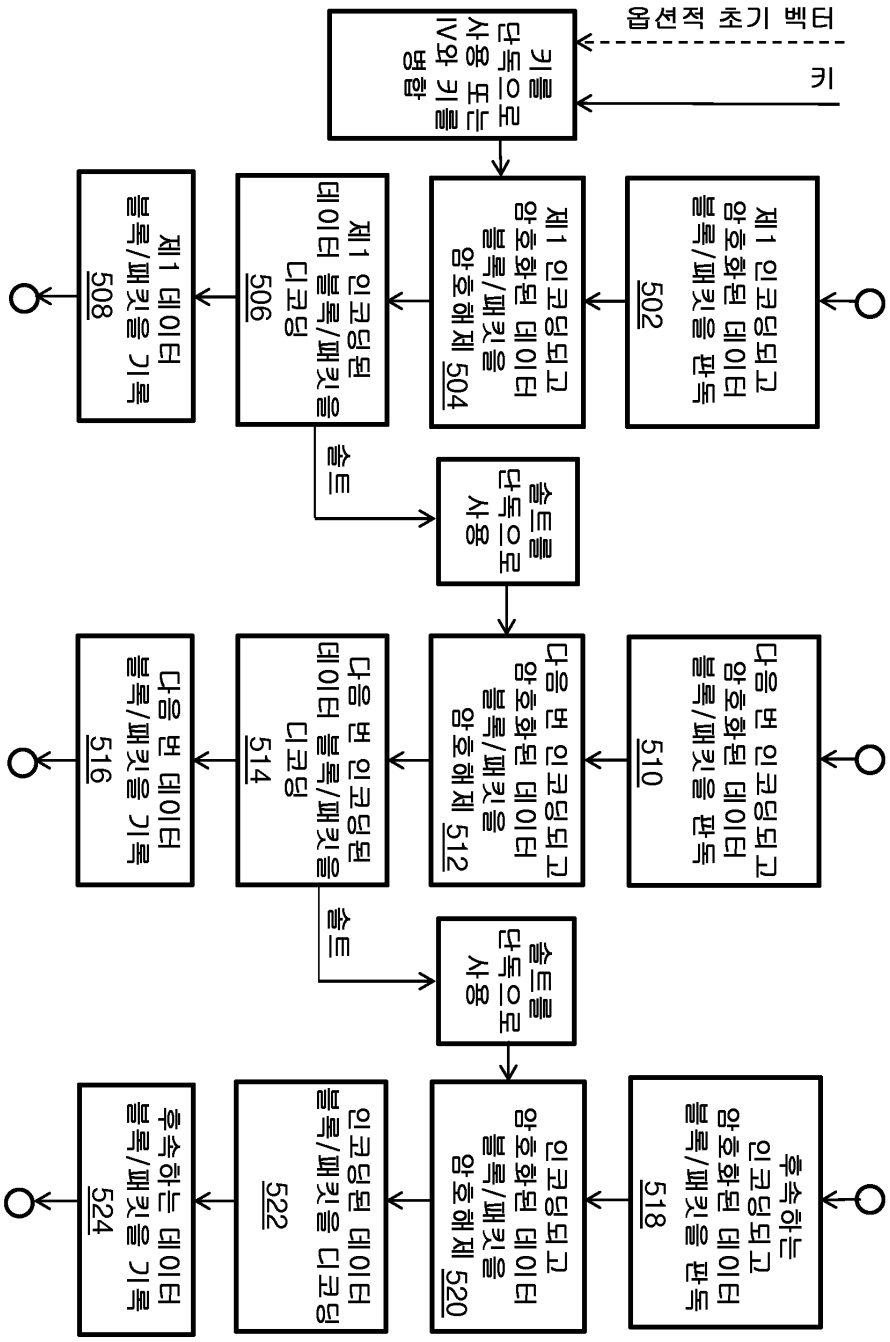
도면3


키를 단독으로 사용 또는 IV와 키를 병합
옵션적 초기 벡터
키
제1 인코딩되고 암호화된 데이터 블록/패킷을 판독 302
제1 인코딩되고 암호화된 데이터 블록/패킷을 암호해제 304
제1 인코딩된 데이터 블록/패킷을 디코딩 306
제1 데이터 블록/패킷을 기록 308
솔트
솔트와 키를 병합
키
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 판독 310
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 암호해제 312
다음 번 인코딩된 데이터 블록/패킷을 디코딩 314
다음 번 데이터 블록/패킷을 기록 316
솔트
솔트와 키를 병합
키
후속하는 인코딩되고 암호화된 데이터 블록/패킷을 판독 318
인코딩되고 암호화된 데이터 블록/패킷을 암호해제 320
인코딩된 데이터 블록/패킷을 디코딩 322
후속하는 데이터 블록/패킷을 기록 324

도면4


옵션적 초기 벡터
키
키를 단독으로 사용 또는 IV와 키를 병합
제1 데이터 블록/패킷을 판독 402
제1 데이터 블록/패킷을 인코딩 404
제1 인코딩된 데이터 블록/패킷을 암호화 406
제1 인코딩되고 암호화된 데이터 블록/패킷을 기록 408
솔트
솔트를 단독으로 사용
다음 번 데이터 블록/패킷을 판독 410
다음 번 데이터 블록/패킷을 인코딩 412
다음 번 인코딩된 데이터 블록/패킷을 암호화 414
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 기록 416
솔트
솔트를 단독으로 사용
후속하는 데이터 블록/패킷을 판독 418
데이터 블록/패킷을 인코딩 420
인코딩된 데이터 블록/패킷을 암호화 422
후속하는 인코딩되고 암호화된 데이터 블록/패킷을 기록 424

도면5


옵션적 초기 벡터
키
키를 단독으로 사용 또는 IV와 키를 병합
제1 인코딩되고 암호화된 데이터 블록/패킷을 판독 502
제1 인코딩되고 암호화된 데이터 블록/패킷을 암호해제 504
제1 인코딩된 데이터 블록/패킷을 디코딩 506
제1 데이터 블록/패킷을 기록 508
출트
출트를 단독으로 사용
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 판독 510
다음 번 인코딩되고 암호화된 데이터 블록/패킷을 암호해제 512
다음 번 인코딩된 데이터 블록/패킷을 디코딩 514
다음 번 데이터 블록/패킷을 기록 516
출트
출트를 단독으로 사용
후속하는 인코딩되고 암호화된 데이터 블록/패킷을 판독 518
인코딩되고 암호화된 데이터 블록/패킷을 암호해제 520
인코딩된 데이터 블록/패킷을 디코딩 522
후속하는 데이터 블록/패킷을 기록 524